

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006215

International filing date: 24 March 2005 (24.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-206335
Filing date: 13 July 2004 (13.07.2004)

Date of receipt at the International Bureau: 28 April 2005 (28.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 7 月 1 3 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 2 0 6 3 3 5

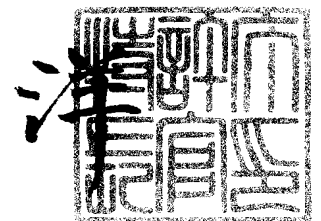
パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号
J P 2 0 0 4 - 2 0 6 3 3 5
The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

出 願 人
Applicant(s): 松下電器産業株式会社

2 0 0 5 年 4 月 1 3 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】	特許願	
【整理番号】	2048160240	
【提出日】	平成16年 7月13日	
【あて先】	特許庁長官 殿	
【国際特許分類】	G09C	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	野仲 真佐男	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	布田 裕一	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	中野 稔久	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	横田 薫	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	大森 基司	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	宮崎 雅也	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	山本 雅哉	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	村瀬 薫	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	小野田 仙一	
【特許出願人】		
【識別番号】	000005821	
【氏名又は名称】	松下電器産業株式会社	
【代理人】		
【識別番号】	100090446	
【弁理士】		
【氏名又は名称】	中島 司朗	
【手数料の表示】		
【予納台帳番号】	014823	
【納付金額】	16,000円	
【提出物件の目録】		
【物件名】	特許請求の範囲 1	
【物件名】	明細書 1	
【物件名】	図面 1	
【物件名】	要約書 1	
【包括委任状番号】	9003742	

【書類名】 特許請求の範囲

【請求項 1】

不正コンテンツを検知する不正コンテンツ検知システムであって、

前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、

前記配布センタは、

前記コンテンツを受け付ける入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成部と、

前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成部と、

前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布部と、を備え、

前記実行装置は、

前記認証情報を検証するための検証情報を保持する検証情報格納部と、

前記検証情報及び前記配布データ領域特定情報を基に、前記認証情報を検証する認証情報検証部と、

前記認証情報検証部での検証結果が正当な場合にのみ、前記取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始する実行部と、

前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記実行部へ渡す取得部と、

を備えることを特徴とする不正コンテンツ検知システム。

【請求項 2】

コンテンツを実行、もしくは再生する実行装置であって、

前記実行装置は、

認証情報を検証するための検証情報を保持する検証情報格納部と、

前記検証情報及び前記コンテンツの領域を特定する配布データ領域特定情報を基に、認証情報を検証する認証情報検証部と、

前記認証情報検証部での検証結果が正当な場合にのみ、取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始する実行部と、

前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記実行部へ渡す取得部と、

を備えることを特徴とする実行装置。

【請求項 3】

前記取得部は、可搬媒体からデータを取得すること、

を特徴とする、請求項 2 に記載の実行装置。

【請求項 4】

前記可搬媒体は光ディスクであり、

前記取得部は、前記光ディスク経由でデータを取得し、

前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の最終物理アドレスを含むこと、

を特徴とする、請求項 3 に記載の実行装置。

【請求項 5】

前記配布データ領域特定情報は、さらに、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の開始物理アドレスを含むこと、

を特徴とする、請求項 4 に記載の実行装置。

【請求項 6】

前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、

を特徴とする、請求項 2 に記載の実行装置。

【請求項 7】

前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を含むデータのデータサイズを含むこと、

を特徴とする、請求項 2 から請求項 6 のいずれか 1 項に記載の実行装置。

【請求項 8】

前記実行装置は、さらに、

コンテンツ鍵を保持するコンテンツ鍵格納部と、を備え、

前記取得部は、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信し、

前記実行部は、前記暗号化コンテンツを復号化すること、

を特徴とする、請求項 2 から請求項 7 のいずれか 1 項に記載の実行装置。

【請求項 9】

前記実行装置は、さらに、

デバイス鍵を保持するデバイス鍵格納部と、

前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、

前記取得部はさらに、前記暗号化鍵束を受信すること、

を特徴とする、請求項 8 に記載の実行装置。

【請求項 10】

前記認証情報は、前記検証対象データに対するデジタル署名であること、

を特徴とする、請求項 2 から請求項 9 のいずれか 1 項に記載の実行装置。

【請求項 11】

前記検証情報は、デジタル署名方式の検証鍵であること、

を特徴とする、請求項 2 から請求項 10 のいずれか 1 項に記載の実行装置。

【請求項 12】

前記認証情報検証部は、前記検証情報及び前記コンテンツの属性値及び前記配布データ領域特定情報を基に、認証情報を検証すること、

を特徴とする、請求項 2 から請求項 11 のいずれか 1 項に記載の実行装置。

【請求項 13】

前記取得部は、さらに、前記コンテンツの属性値を取得すること、

を特徴とする、請求項 12 に記載の実行装置。

【請求項 14】

前記コンテンツは、前記実行装置で実行可能なプログラムであり、

前記実行部は、前記プログラムを実行すること、

を特徴とする請求項 2 から請求項 13 のいずれか 1 項に記載の実行装置。

【請求項 15】

コンテンツを配布する配布センタであって、

前記配布センタは、

前記コンテンツを受け付ける入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成部と、

前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成部と、

前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布

する配布部と、を備え、
を備えることを特徴とする配布センタ。

【請求項 16】

前記配布部は、可搬媒体へデータを記録すること、
を特徴とする、請求項 15 に記載の配布センタ。

【請求項 17】

前記可搬媒体は光ディスクであり、
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の最終物理アドレスを含むこと、
を特徴とする、請求項 16 に記載の配布センタ。

【請求項 18】

前記配布データ領域特定情報は、さらに、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の開始物理アドレスを含むこと、
を特徴とする、請求項 17 に記載の配布センタ。

【請求項 19】

前記配布部は、記録媒体、もしくは通信ネットワーク、もしくは放送網を介してデータを配布すること、
を特徴とする、請求項 15 に記載の実行装置。

【請求項 20】

前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を含むデータのデータサイズを含むこと、
を特徴とする、請求項 15 から請求項 19 のいずれか 1 項に記載の実行装置。

【請求項 21】

前記配布センタはさらに、
コンテンツ鍵を保持するコンテンツ鍵格納部と、
前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する暗号化部と、を備え、
前記配布部は、前記コンテンツの代わりに前記暗号化コンテンツを配布すること、
を特徴とする、請求項 15 から請求項 20 のいずれか 1 項に記載の配布センタ。

【請求項 22】

前記配布センタはさらに
一以上のデバイス鍵を保持する実行装置情報格納部と、
前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、
前記配布部はさらに、前記暗号化鍵束を配布すること、
を特徴とする、請求項 21 に記載の配布センタ。

【請求項 23】

前記認証情報は、前記検証対象データに対するデジタル署名であること、
を特徴とする、請求項 15 から請求項 22 のいずれか 1 項に記載の配布センタ。

【請求項 24】

前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、
を特徴とする、請求項 15 から請求項 23 のいずれか 1 項に記載の配布センタ。

【請求項 25】

前記認証情報生成部は、認証情報生成情報を基に、前記配布データ領域特定情報及び前記コンテンツの属性値を含む検証対象データに対する認証情報を生成すること、
を特徴とする、請求項 15 から請求項 24 のいずれか 1 項に記載の配布センタ。

【請求項 26】

前記配布部は、さらに、前記コンテンツの属性値を配布すること、
を特徴とする、請求項 25 に記載の配布センタ。

【請求項 27】

前記コンテンツはプログラムであること、
を特徴とする請求項 15 から請求項 26 のいずれか 1 項に記載の配布センタ。

【請求項 28】

不正コンテンツを検知する不正コンテンツ検知方法であって、
前記不正コンテンツ検知方法は、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布手段と、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行手段と、から構成され、
前記配布手段は、
前記コンテンツを受け付ける入力手段と、
認証情報生成情報を保持する認証情報生成情報格納手段と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成手段と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成手段と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布手段と、を備え、
前記実行手段は、
前記認証情報を検証するための検証情報を保持する検証情報格納手段と、
前記検証情報及び前記配布データ領域特定情報を基に、前記認証情報を検証する認証情報検証手段と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始するコンテンツ実行手段と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記コンテンツ実行手段へ渡す取得手段と、
を備えることを特徴とする不正コンテンツ検知方法。

【請求項 29】

コンテンツを実行、もしくは再生する実行方法であって、
前記実行方法は、
認証情報を検証するための検証情報を保持する検証情報格納手段と、
前記検証情報及び前記コンテンツの領域を特定する配布データ領域特定情報を基に、認証情報を検証する認証情報検証手段と、
前記認証情報検証部での検証結果が正当な場合にのみ、取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始するコンテンツ実行手段と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記コンテンツ実行手段へ渡す取得手段と、
を備えることを特徴とする実行方法。

【請求項 30】

コンテンツを配布する配布方法であって、
前記配布方法は、
前記コンテンツを受け付ける入力手段と、
認証情報生成情報を保持する認証情報生成情報格納手段と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成手段と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成手段と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布手段と、を備え、

を備えることを特徴とする配布方法。

【書類名】 明細書

【発明の名称】 不正コンテンツ検知システム

【技術分野】

【0001】

本発明は不正なコンテンツを検知する技術に関するものである。

【背景技術】

【0002】

近年、デジタルコンテンツの普及に伴い、例えば著作権を保持する者以外がデジタルコンテンツを不正に販売する、いわゆる不正コンテンツ（違法コンテンツ）の配布が社会問題となってきた。この不正コンテンツ配布の一つのケースとして、映画館等で上映される映画コンテンツを、例えば著作権を保持しない第三者がデジタルビデオカメラ等で盗撮し、その盗撮した不正動画コンテンツを光ディスクに記録し販売するというものが挙げられる。また別のケースとして、正規に販売されている片面2層DVD-ROMディスク（最大8.5ギガバイト）に記録されているDVD-VIDEO形式の映画コンテンツの画質を4.7ギガバイト以下に収まるように変換処理をして不正コンテンツを生成して、その不正コンテンツを片面1層DVD-Rディスク（最大4.7ギガバイト）に記録して販売するものも挙げられる。

【0003】

上記のような不正コンテンツ配布（不正コンテンツ利用）を防ぐ方法の従来技術としては、特許文献1に記載されている不正コンテンツ検知システムと自明な方式が知られている。

特許文献1に記載の従来技術は、可搬媒体の中に、複数のコンテンツブロック（部分コンテンツ）から構成されるコンテンツデータの他に、複数のコンテンツブロックに対応するハッシュ値と、複数のハッシュ値を結合したデータに対する著作権者のデジタル署名と、を記録しておく。そして、実行装置では、可搬媒体の中のコンテンツを再生する前に、記録されたハッシュ値が正規の著作権者によって記録されたものか、デジタル署名を用いて検証を行う。そして、検証が失敗したら、コンテンツの再生開始をしない。また、コンテンツを再生している途中にも、記録されたハッシュ値がコンテンツデータの正しいハッシュ値なのか検証を行う。そして、検証が失敗したら、コンテンツの再生を停止するものである。こうすることにより、正規の著作権者でない第三者が不正コンテンツを可搬媒体に記録して配布したとしても、実行装置ではその不正コンテンツを再生開始しないか、途中で再生を停止する。これにより、不正なコンテンツの配布防止につながる。

【0004】

ここでは、特許文献1に記載の従来技術の詳細の一例について図35を用いて説明する。前提として、正規の著作権者はデジタル署名を作成するための署名生成鍵を有しており、実行装置はその署名生成鍵に対応する署名検証鍵を有しているとする。初めに、正規の著作権者が、コンテンツデータと、複数のコンテンツブロックに対応するハッシュ値と、複数のハッシュ値を結合したデータに対するデジタル署名と、を記録した可搬媒体を生成する場合の動作について説明する。まず、デジタルコンテンツをn個（nは2以上の自然数）のコンテンツブロック（図37のコンテンツブロックBLK1・・・BLKnに対応）に分割する。そして、一方向性関数を用いてコンテンツブロックBLK1のハッシュ値HASH1を計算する。コンテンツブロックBLK2以降も同様にハッシュ値を計算し、それぞれのコンテンツブロックBLK2、・・・、BLKnに対応するハッシュ値HASH2、・・・、HASHnを求める。そして、n個のハッシュ値HASH1、・・・、HASHnを連結させたものをヘッダ情報とする。その後、正規の著作権者の署名生成鍵を用いて、そのヘッダ情報のデジタル署名を生成し、そのデジタル署名とヘッダ情報とコンテンツを可搬媒体に記録し、実行装置へ提供する。続いて、実行装置が、提供された可搬媒体内のコンテンツを再生する場合の動作について説明する。まず、署名検証鍵を用いてデジタル署名が正規の著作権者によるヘッダ情報のデジタル署名であるかを検証する。そこで、もし正規のデジタル署名であることが確認されれば、コンテンツの再生を開始す

る。その後、実行装置はコンテンツを再生しながら、再生しているコンテンツブロックのハッシュ値を計算し続ける。そして、次のコンテンツブロックに再生位置が移動する際に、計算したハッシュ値がヘッダ情報のハッシュ値と一致するかを確認し、もし一致しなかった場合、コンテンツの再生を停止する。このような特許文献1に記載の従来技術により、何らかの理由によりコンテンツが盗み出され、例えば著作権を保持しない者がそのコンテンツを可搬媒体に記録して配布、販売しようとしても、可搬媒体には著作権者のデジタル署名が記録されていないため、実行装置ではそのコンテンツを再生開始しないか、もしくは、途中で再生が停止する。これにより、不正コンテンツ流通に対する対策が可能となる。

【0005】

この特許文献1に記載の従来技術の課題は、実行装置がコンテンツを再生している間、継続してコンテンツブロックのハッシュ値を計算し続けなければならないので、コンテンツ再生中の実行装置の処理負荷が高いという点である。例えば、一般に、コンテンツは暗号化されて配布されるため、再生する直前にコンテンツを復号化する必要がある。このような場合、コンテンツを復号化すると同時に、復号化したコンテンツのハッシュ値を計算しなければならないという課題があった。

【0006】

上記に記載の課題を解決するものとして自明な方式が挙げられる。自明な方式では、可搬媒体の中に、コンテンツデータの他に、そのコンテンツデータに対するデジタル署名を記録しておく。そして、実行装置では、記録されたデジタル署名がコンテンツデータに対する著作権者の正規のデジタル署名であることが検証された場合に、可搬媒体の中のコンテンツを再生する。こうすることにより、正規の著作権者でない第三者が映画館等において盗撮したコンテンツを可搬媒体に記録して販売したとしても、その可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置はコンテンツを再生しない。これにより、不正なコンテンツの配布防止につながる。

【特許文献1】 米国特許第6480961号明細書

【特許文献2】 特開2002-281013号公報

【非特許文献1】 「情報セキュリティ」宮地充子・菊池浩明編著 情報処理学会編集

【非特許文献2】 「THE ART OF COMPUTER PROGRAMMING Vol. 2 ~ SEMINUMERICAL ALGORITHMS」 DONALD E. KNUTH 著、ISBN 0-201-03822-6

【非特許文献3】 「Protocols for Authentication and Key Establishment」 Colin Boyd/Anish Mathuria 著、ISBN 3-540-43107-1

【発明の開示】

【発明が解決しようとする課題】

【0007】

ここでは、不正コンテンツが配布される別の形態として、正規の著作権者により配布された可搬媒体に記録可能なデータ領域が残っている場合、著作権を保持しない不正者によってその記録可能なデータ領域に不正コンテンツが記録（追記）されるという不正行為を想定する。また、別の形態として、著作権を保持しない不正者によって、正規の著作権者により配布された可搬媒体に記録されている全データを別の可搬媒体（前の可搬媒体と同じデータサイズを記録可能な可搬媒体であってもよいし、前の可搬媒体以上のデータサイズを記録可能な可搬媒体であってもよい）にコピーして、その別の可搬媒体で記録可能なデータ領域に不正コンテンツが記録（追記）されるという不正行為も想定する。このような場合、上記で説明した自明な方式における実行装置では、正規の著作権者により記録された認証情報により認証が成功してしまうことで、コンテンツの実行、再生を開始してしまい、最終的には可搬媒体に記録された不正コンテンツも実行、再生出来てしまうことになる。

【０００８】

本発明は、前記従来技術（自明な方式）の課題を解決するもので、可搬媒体に著作権を保持しない不正者によって不正コンテンツが記録されたとしても、実行装置はその可搬媒体に記録されているコンテンツが著作権を保持しない不正者によって記録されたことを検知可能な不正コンテンツ検知システムを提供することを目的とする。

【課題を解決するための手段】

【０００９】

上記課題を解決するために、請求項１における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、

前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、

前記配布センタは、

前記コンテンツを受け付ける入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成部と、

前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成部と、

前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布部と、を備え、

前記実行装置は、

前記認証情報を検証するための検証情報を保持する検証情報格納部と、

前記検証情報及び前記配布データ領域特定情報を基に、前記認証情報を検証する認証情報検証部と、

前記認証情報検証部での検証結果が正当な場合にのみ、前記取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始する実行部と、

前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記実行部へ渡す取得部と、

を備えることを特徴とする。

【００１０】

請求項２における発明は、コンテンツを実行、もしくは再生する実行装置であって、

前記実行装置は、

認証情報を検証するための検証情報を保持する検証情報格納部と、

前記検証情報及び前記コンテンツの領域を特定する配布データ領域特定情報を基に、認証情報を検証する認証情報検証部と、

前記認証情報検証部での検証結果が正当な場合にのみ、取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始する実行部と、

前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記実行部へ渡す取得部と、

を備えることを特徴とする。

【００１１】

請求項３における発明は、請求項２に記載の実行装置であって、

前記取得部は、可搬媒体からデータを取得すること、

を特徴とする。

請求項４における発明は、請求項３に記載の実行装置であって、

前記可搬媒体は光ディスクであり、

前記取得部は、前記光ディスク経由でデータを取得し、

前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の最終物理アドレスを含むこと、

を特徴とする。

【００１２】

請求項５における発明は、請求項４に記載の実行装置であって、

前記配布データ領域特定情報は、さらに、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の開始物理アドレスを含むこと、

を特徴とする。

請求項６における発明は、請求項２に記載の実行装置であって、

前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、

を特徴とする。

【００１３】

請求項７における発明は、請求項２から請求項６のいずれか１項に記載の実行装置であって、

前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を含むデータのデータサイズを含むこと、

を特徴とする。

【００１４】

請求項８における発明は、請求項２から請求項７のいずれか１項に記載の実行装置であって、

前記実行装置は、さらに、

コンテンツ鍵を保持するコンテンツ鍵格納部と、を備え、

前記取得部は、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信し、

前記実行部は、前記暗号化コンテンツを復号化すること、

を特徴とする。

【００１５】

請求項９における発明は、請求項８に記載の実行装置であって、

前記実行装置は、さらに、

デバイス鍵を保持するデバイス鍵格納部と、

前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、

前記取得部はさらに、前記暗号化鍵束を受信すること、

を特徴とする。

【００１６】

請求項１０における発明は、請求項２から請求項９のいずれか１項に記載の実行装置であって、

前記認証情報は、前記検証対象データに対するデジタル署名であること、

を特徴とする。

請求項１１における発明は、請求項２から請求項１０のいずれか１項に記載の実行装置であって、

前記検証情報は、デジタル署名方式の検証鍵であること、

を特徴とする。

【００１７】

請求項１２における発明は、請求項２から請求項１１のいずれか１項に記載の実行装置であって、

前記認証情報検証部は、前記検証情報及び前記コンテンツの属性値及び前記配布データ領域特定情報を基に、認証情報を検証すること、

を特徴とする。

【００１８】

請求項１３における発明は、請求項１２に記載の実行装置であって、前記取得部は、さらに、前記コンテンツの属性値を取得すること、を特徴とする。

請求項１４における発明は、請求項２から請求項１３のいずれか１項に記載の実行装置であって、

前記コンテンツは、前記実行装置で実行可能なプログラムであり、前記実行部は、前記プログラムを実行すること、を特徴とする。

【００１９】

請求項１５における発明は、コンテンツを配布する配布センタであって、前記配布センタは、

前記コンテンツを受け付ける入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成部と、

前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成部と、

前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布部と、を備え、

を備えることを特徴とする。

【００２０】

請求項１６における発明は、請求項１５に記載の配布センタであって、

前記配布部は、可搬媒体へデータを記録すること、

を特徴とする。

請求項１７における発明は、請求項１６に記載の配布センタであって、

前記可搬媒体は光ディスクであり、

前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の最終物理アドレスを含むこと、

を特徴とする。

【００２１】

請求項１８における発明は、請求項１７に記載の配布センタであって、

前記配布データ領域特定情報は、さらに、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の開始物理アドレスを含むこと、

を特徴とする。

請求項１９における発明は、請求項１５に記載の実行装置であって、

前記配布部は、記録媒体、もしくは通信ネットワーク、もしくは放送網を介してデータを配布すること、

を特徴とする。

【００２２】

請求項２０における発明は、請求項１５から請求項１９のいずれか１項に記載の実行装置であって、

前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を含むデータのデータサイズを含むこと、

を特徴とする。

【００２３】

請求項２１における発明は、請求項１５から請求項２０のいずれか１項に記載の配布センタであって、

前記配布センタはさらに、

コンテンツ鍵を保持するコンテンツ鍵格納部と、
前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する暗号化部と、を備え、
前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、
を特徴とする。

【００２４】

請求項２２における発明は、請求項２１に記載の配布センタであって、
前記配布センタはさらに
一以上のデバイス鍵を保持する実行装置情報格納部と、
前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、
前記配布部はさらに、前記暗号化鍵束を配布すること、
を特徴とする。

【００２５】

請求項２３における発明は、請求項１５から請求項２２のいずれか１項に記載の配布センタであって、
前記認証情報は、前記検証対象データに対するデジタル署名であること、
を特徴とする。
請求項２４における発明は、請求項１５から請求項２３のいずれか１項に記載の配布センタであって、
前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、
を特徴とする。

【００２６】

請求項２５における発明は、請求項１５から請求項２４のいずれか１項に記載の配布センタであって、
前記認証情報生成部は、認証情報生成情報を基に、前記配布データ領域特定情報及び前記コンテンツの属性値を含む検証対象データに対する認証情報を生成すること、
を特徴とする。

【００２７】

請求項２６における発明は、請求項２５に記載の配布センタであって、
前記配布部は、さらに、前記コンテンツの属性値を配布すること、
を特徴とする。
請求項２７における発明は、請求項１５から請求項２６のいずれか１項に記載の配布センタであって、
前記コンテンツはプログラムであること、
を特徴とする。

【００２８】

請求項２８における発明は、不正コンテンツを検知する不正コンテンツ検知方法であって、
前記不正コンテンツ検知方法は、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布手段と、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行手段と、から構成され、
前記配布手段は、
前記コンテンツを受け付ける入力手段と、
認証情報生成情報を保持する認証情報生成情報格納手段と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成手段と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成手段と、

前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布手段と、を備え、

前記実行手段は、

前記認証情報を検証するための検証情報を保持する検証情報格納手段と、

前記検証情報及び前記配布データ領域特定情報を基に、前記認証情報を検証する認証情報検証手段と、

前記認証情報検証部での検証結果が正当な場合にのみ、前記取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始するコンテンツ実行手段と、

前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記コンテンツ実行手段へ渡す取得手段と、

を備えることを特徴とする。

【0029】

請求項29における発明は、コンテンツを実行、もしくは再生する実行方法であって、前記実行方法は、

認証情報を検証するための検証情報を保持する検証情報格納手段と、

前記検証情報及び前記コンテンツの領域を特定する配布データ領域特定情報を基に、認証情報を検証する認証情報検証手段と、

前記認証情報検証部での検証結果が正当な場合にのみ、取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始するコンテンツ実行手段と、

前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記コンテンツ実行手段へ渡す取得手段と、

を備えることを特徴とする。

【0030】

請求項30における発明は、コンテンツを配布する配布方法であって、

前記配布方法は、

前記コンテンツを受け付ける入力手段と、

認証情報生成情報を保持する認証情報生成情報格納手段と、

前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成手段と、

前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成手段と、

前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布手段と、を備え、

を備えることを特徴とする。

【発明の効果】

【0031】

不正コンテンツが配布される別の形態として、正規の著作権者により配布された可搬媒体に記録可能なデータ領域が残っている場合、著作権を保持しない不正者によってその記録可能なデータ領域に不正コンテンツが記録（追記）されるという場合がありうる。また、別の形態として、著作権を保持しない不正者によって、正規の著作権者により配布された可搬媒体に記録されている全データを別の可搬媒体にコピーして、その別の可搬媒体で記録可能なデータ領域に不正コンテンツが記録（追記）されるという場合がありうる。このような場合、実行装置においては、正規の著作権者により記録されたデータ（認証情報など）により認証が成功してしまうことで、コンテンツの実行、再生を開始してしまい、最終的には可搬媒体に記録された不正コンテンツも実行、再生出来てしまうことも想定される。上記のような形態を鑑み、本発明の不正コンテンツ検知システムでは、さらに、可搬媒体の中に、可搬媒体に記録されているデータの領域を識別する配布データ領域特

定情報（例えば、データが記録されている開始物理アドレスと最終物理アドレス、もしくは、記録データサイズなど）と、その配布データ領域特定情報に対する著作権者の認証情報（例えば、デジタル署名。属性値に対するデジタル署名と兼ねてもよい）とを記録しておく。そして、実行装置の取得部では、可搬媒体に記録された配布データ領域特定情報を受け取った場合、その配布データ領域特定情報で指定された領域外のデータは取得部の外部からの要求でも取得しないようにする。このようにすることによって、正規の著作権者により配布された可搬媒体に記録可能なデータ領域が残っている場合に、著作権を保持しない不正者によってその記録可能なデータ領域に不正コンテンツが記録されたとしても、取得部は予め著作権者によって指定された領域外のデータは取得しないため、不正コンテンツを実行、再生出来ないようになる。また、実行装置では、さらに、可搬媒体に記録された配布データ領域特定情報が著作権者によって記録されたものかどうか、認証情報を基に検証し、検証が失敗した場合、該当する可搬媒体に記録されているコンテンツは実行開始、再生開始しないようにした。そうすることによって、著作権が保持しない不正者が、可搬媒体の記録されている配布データ領域特定情報を改ざんしたとしても、その可搬媒体に記録されているコンテンツは実行、再生しないようになった。このことにより、著作権を保持しない不正者によって不正コンテンツが記録（追記）されるという不正行為を防ぐことが出来るようになった。

【0032】

また、実行装置において、配布された不正コンテンツが実行、再生される不正行為の別の形態として、可搬媒体に記録されているデータを読み出すドライブ部と、ドライブ部によって取得されたデータを実行、再生するコンテンツ実行部との間に流れるデータを改竄される場合がある。例えば、著作権を保持しない不正者は、正規の著作権者による配布データ領域特定情報と対応する認証情報を取得しているものとする。その場合、その不正者は、不正な可搬媒体に、任意の配布データ領域特定情報と、偽の認証情報とを記録する。それにより、実行装置のドライブ部においては、その不正な可搬媒体に記録されている配布データ領域特定情報を基にして、その配布データ領域特定情報で指定された領域のデータはコンテンツ実行部からの要求で取得出来るようになる。続いて、実行装置のドライブ部が、その不正な可搬媒体に記録されている配布データ領域特定情報と、その配布データ領域特定情報に対する認証情報をコンテンツ実行部へ出力しようとする。その際、不正者は、ドライブ部が出力した配布データ領域特定情報と認証情報を、正規の著作権者による配布データ領域特定情報と対応する認証情報に差し替えて、コンテンツ実行部へ出力する。それにより、コンテンツ実行部では、正規の著作権者による配布データ領域特定情報と対応する認証情報を基に暗号化コンテンツの検証を行うため、検証が成功する。よって、コンテンツ実行部はコンテンツの実行、再生を開始してしまう。上記のような不正行為を鑑み、本発明の不正コンテンツ検知システムでは、ドライブ部からコンテンツ実行部へ出力するデータの一部（例えば、配布データ領域特定情報）を暗号化して出力するようにした。これにより、不正者は、ドライブ部が出力したデータを別のデータに差し替えてコンテンツ実行部へ出力しようとしても、不正者は正しく暗号化することが出来ないため、正しくコンテンツ実行部へ出力できなくなった。この際、同じデータであっても、ドライブ部からコンテンツ実行部へ出力する暗号文が異なるようにしてもよい。これは、例えば、ドライブ部とコンテンツ実行部が毎回異なるセッション鍵を共有することにより実現出来る。このことにより、著作権を保持しない不正者によって不正コンテンツが実行、再生されるという不正行為を防ぐことが出来るようになった。

【発明を実施するための最良の形態】

【0033】

以下本発明の実施の形態について、図面を参照しながら説明する。

（実施の形態1）

著作権を保持しない不正者により、不正コンテンツが記録された可搬媒体が配布された場合に、実行装置では不正者により配布された可搬媒体に記録されている不正コンテンツ

が実行、再生出来ないようにすることが望まれる。このように、不正者により不正コンテンツが記録された可搬媒体が配布される不正行為には、例えば、以下で示すような不正行為が挙げられる。その不正行為は、不正者が、正規の配布センタによって配布された可搬媒体に記録されているコンテンツの全部を新たな可搬媒体へ記録して、さらに、その新たな可搬媒体の記録されていない部分に不正コンテンツを記録する不正行為である。その不正行為においては、新たな可搬媒体には、正規の配布センタによって配布されたデータがそのまま記録されているため、新たな可搬媒体には著作権者によって記録されたコンテンツが格納されていると判断してしまう場合がある。これを利用して、不正者は実行装置で不正コンテンツを実行、再生させることを試みるという不正行為である。本発明の実施の形態１では、上記の不正行為を想定し、そのような不正コンテンツが記録された可搬媒体が配布された場合にでも、実行装置では不正者により配布された可搬媒体に記録されている不正コンテンツが実行、再生出来ないようにすることを目的とする。

【００３４】

本発明の実施の形態１では、上記不正行為に対する対策として、配布センタは、著作権者によって可搬媒体に記録されたデータのデータ領域の領域である配布データ領域特定情報を記録するようにして、実行装置では、その配布データ領域特定情報で指定されたデータ領域の領域外にあるデータは取得しないようにした。このことにより、実行装置では配布データ領域特定情報により予め著作権者によって指定された領域外のデータは取得しないため、可搬媒体に格納されている不正コンテンツを実行、再生出来ないようになる。また可搬媒体には、さらに、配布データ領域特定情報に対する認証情報を記録するようにして、実行装置では、認証情報が可搬媒体に記録された配布データ領域特定情報に対する正規の著作権者の認証情報であるか検証し、検証が成功した場合にのみ、コンテンツの実行、再生を行うようにした。このことにより、著作権を保持しない不正者が、可搬媒体の記録されている配布データ領域特定情報を改ざんしたとしても、その可搬媒体に記録されているコンテンツは実行、再生しないようになった。このことにより、上記不正行為に対する耐性を向上させる。

【００３５】

図１は、本発明の実施の形態１における不正コンテンツ検知システムの構成図である。図１において、配布センタ１０は外部からコンテンツＣＮＴを受け取り、後述する実行装置１２がコンテンツＣＮＴを実行するために必要となる情報を後述する可搬媒体１１に記録するものであり、可搬媒体１１は実行装置１２がコンテンツＣＮＴを実行するために必要となる情報が記録されているものであり、複数の実行装置１２は可搬媒体１１に記録されている情報を用いて、コンテンツＣＮＴを実行するものである。

【００３６】

不正コンテンツ検知システム１は、配布センタ１０（正規のコンテンツ提供者、著作権者、正規の光ディスクプレス業者など）が、ＤＶＤ（Digital Versatile Disc）等の可搬媒体１１の配布手段によって、暗号化されたコンテンツＣＮＴである暗号化コンテンツＥＮＣＣＮＴと、暗号化コンテンツＥＮＣＣＮＴを基に生成される第一ハッシュテーブル群HASH TBL １Ｇと第二ハッシュテーブルHASH TBL ２とコンテンツ位置情報POSと、可搬媒体１１に記録されたデータのデータ領域の領域である配布データ領域特定情報AREAと、第二ハッシュテーブルHASH TBL ２とコンテンツ位置情報POSと配布データ領域特定情報AREAの正当性を示す情報である認証情報AUTHを、各実行装置１２へ配布する。各実行装置１２は、暗号化コンテンツＥＮＣＣＮＴを基に第一ハッシュテーブル群HASH TBL １Ｇと第二ハッシュテーブルHASH TBL ２の一部の情報を入れ替えて入替第二ハッシュテーブルREPHASH TBL ２を作成し、認証情報AUTHが配布センタ１０による入替第二ハッシュテーブルREPHASH TBL ２とコンテンツ位置情報POSと配布データ領域特定情報AREAの正規の認証情報であることを確認し、コンテンツＣＮＴを実行開始する。

【００３７】

以上が、本実施の形態の概要である。以下に、本発明の不正コンテンツ検知システムの

一実施の形態である不正コンテンツ検知システム１の詳細について説明を行う。

＜不正コンテンツ検知システム１の構成＞

不正コンテンツ検知システム１は、図１に示すように、配布センタ１０と、可搬媒体１１と、 s 個の実行装置１２（ s は１以上の自然数）から構成される。

【００３８】

以下に、これらの構成要素について、詳細に説明する。まず、配布センタ１０の構成と動作について述べ、続いて可搬媒体１１の構成について述べ、最後に実行装置１２の構成と動作について述べる。

＜配布センタ１０の構成＞

配布センタ１０は、図２に示すように、入力部１００１、コンテンツ鍵生成部１００２、実行装置情報格納部１００３、暗号化鍵束生成部１００４、暗号化部１００５、ハッシュテーブル生成部１００６、可搬媒体イメージ生成部１００７、配布データ領域特定情報生成部１００８、認証情報生成情報格納部１００９、認証情報生成部１０１０、記録部１０１１から構成される。

【００３９】

（１）入力部１００１

入力部１００１は、外部からコンテンツＣＮＴを入力出来るものである。入力部１００１は、例えば、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭやビデオテープ、映画フィルム等からコンテンツＣＮＴを読み取る機能を有する。コンテンツＣＮＴは、例えば、ＭＰＥＧ（Moving Picture Experts Group）２フォーマット形式による動画データやＭＰ３フォーマットによる音声データである。外部からコンテンツＣＮＴが入力された場合、コンテンツ鍵生成要求REQをコンテンツ鍵生成部１００２へ出力し、コンテンツＣＮＴを暗号化部１００５へ出力する。なお、外部から入力されるコンテンツＣＮＴは、実行装置１２で実行可能なフォーマット形式であるとしたが、これに限るものではない。例えば、実行装置１２で実行可能なフォーマット形式ではない場合、入力部１００１は、実行装置１２で実行可能なフォーマット形式への変換処理を実施するようにしてもよい。

【００４０】

（２）コンテンツ鍵生成部１００２

コンテンツ鍵生成部１００２は、入力部１００１からコンテンツ鍵生成要求REQが入力された場合、コンテンツ鍵CKを生成する。コンテンツ鍵CKを生成する方法としては、例えば、乱数を用いて１２８ビット鍵データをランダムに生成する方法などがあり、これはコンテンツ鍵生成部１００２が乱数生成手段を有していることにより実現出来る。乱数を生成する方法については、非特許文献２が詳しい。そして、コンテンツ鍵CKを暗号化鍵束生成部１００４及び暗号化部１００５へ出力する。なお、コンテンツ鍵CKはコンテンツＣＮＴを暗号化、復号化するための鍵であり、暗号化部１００５及び実行装置１２の実行部１２１７で利用される。

【００４１】

（３）実行装置情報格納部１００３

実行装置情報格納部１００３は、複数の実行装置１２に与えられる鍵情報を保持するものである。図３は、実行装置情報格納部１００３の一例を示しており、装置識別子AID１に対応付けられたデバイス鍵DK１と、装置識別子AID２に対応付けられたデバイス鍵DK２と、・・・、装置識別子AID s に対応付けられたデバイス鍵DK s を保持している状態を示している。ここで、装置識別子AID１、AID２、・・・、AID s のそれぞれは、複数の実行装置１２のいずれかに対応付けられており、デバイス鍵DK１、DK２、・・・、DK s のそれぞれは、対応する実行装置１２のデバイス鍵格納部１２１１に格納されている鍵である。なお、デバイス鍵DK１、DK２、・・・、DK s のそれぞれはコンテンツ鍵CKを暗号化、復号化するための鍵であり、暗号化鍵束生成部１００４及びコンテンツ鍵取得部１２１２で用いられる。例えば、装置識別子AID１、AID２、・・・、AID s は、それぞれ異なる自然数１、２、・・・、 n であり、デバイス鍵D

K1、DK2、・・・、DKsは、例えば、それぞれ異なる128ビット鍵データである。

【0042】

(4) 暗号化鍵束生成部1004

暗号化鍵束生成部1004は、コンテンツ鍵生成部1002からコンテンツ鍵CKが入力された場合、実行装置情報格納部1003にアクセスして複数の実行装置12が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵CKとを基に、暗号化鍵束KBを生成する。暗号化鍵束KBは、各実行装置12がその暗号化鍵束KBと自身の保持する鍵を用いてコンテンツ鍵CKが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置12はそれぞれ、AID1からAIDsのいずれかの装置識別子と対応するデバイス鍵(DK1、・・・、DKsのいずれか)を保持しており、実行装置情報格納部1003には、図3のように、実行装置12が保持する装置識別子(AID1、・・・、AIDs)と対応するデバイス鍵(DK1、・・・、DKs)の組が全て格納されているとする。そのような場合、暗号化鍵束KBは例えば以下のように生成される。実行装置情報格納部1003から装置識別子AID1と対応するデバイス鍵DK1を取得する。そして、デバイス鍵DK1を基にコンテンツ鍵CKを暗号化し、暗号化コンテンツ鍵ENCK1=Enc(DK1、CK)を生成し、装置識別子AID1に対応付ける。なお、Enc(K、P)を平文Pを暗号化鍵Kで暗号化した際の暗号文とし、以後同じ表記を用いる。そして、他の装置識別子(AID2、・・・、AIDs)とデバイス鍵(DK2、・・・、DKs)に対しても同様の処理を行い、暗号化コンテンツ鍵ENCK2=Enc(DK2、CK)、・・・、ENCKn=Enc(DKs、CK)を生成し、装置識別子AID2、・・・、AIDsに対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵のs組から構成される、図4のような暗号化鍵束KBを生成する。暗号化鍵束KBをこのような構成にすることによって、各実行装置12はその暗号化鍵束KBと自身の保持するデバイス鍵(DK1、・・・、DKsの何れか)を用いてコンテンツ鍵CKが取得出来るようになる。そして、暗号化鍵束KBを可搬媒体イメージ生成部1011に出力する。なお、特許文献2などに記載の方法を用いることで、暗号化鍵束KBの中の暗号化コンテンツ鍵(先程の例ではs個)の数を減らしたり、ある特定の実行装置では正しいコンテンツ鍵CKを取得出来ないようにして、特定の実行装置を無効化することも出来る。また、暗号化鍵束生成部1004で使用する暗号アルゴリズムは、例えば、非特許文献1に記載のAES方式(128ビット鍵)などであり、実行装置12のコンテンツ鍵取得部1212と同じ暗号アルゴリズムを用いる。

【0043】

(5) 暗号化部1005

暗号化部1005は、入力部1001からコンテンツCNTを入力され、さらに、コンテンツ鍵生成部1002からコンテンツ鍵CKとが入力された場合、以下のようにして暗号化コンテンツENCNTを生成する。ここで、コンテンツCNTは、図5で示すように、n個(nは2以上の自然数)の部分コンテンツCNT#1、CNT#2、CNT#3、・・・、CNT#nから構成されるとする。コンテンツCNTがn個の部分コンテンツから構成されている一例としては、コンテンツCNTが複数のファイルから構成されている場合が挙げられる。例えば、コンテンツCNTがDVD-VIDEO形式の動画コンテンツの場合の、VOB(Video Object)ファイル等で分割されている。また、コンテンツCNTが複数のMPEG2形式の動画コンテンツから構成されている場合や、複数のMP3形式の音声コンテンツから構成されている場合もある。なお、DVD-Video形式については、HYPERLINK "例えばインターネットアドレス<http://positron.jfet.org/dvdvideo.html>" 例えばインターネットアドレス<http://positron.jfet.org/dvdvideo.html>に記載されており、MPEG形式については、例えばインターネットアドレスHYPERLINK "<http://www.pioneer.co.jp/crdl/tech/mpeg/l.html>" <http://www.pioneer.co.jp/crdl/tech/mpeg/l.html>に記載されている。

【0044】

そして、コンテンツ鍵CKを用いて部分コンテンツCNT#1を暗号化し、暗号化部分コンテンツENCNT#1=Enc(CK、CNT#1)を生成する。続いて、同じコンテンツ鍵CKを用いて部分コンテンツCNT#2を暗号化し、暗号化部分コンテンツENCNT#2=Enc(CK、CNT#2)を生成する。これを繰り返して、図5で示すようなn個の暗号化部分コンテンツENCNT#1、・・・、ENCNT#nから構成される暗号化コンテンツENCNTを生成する。暗号化部1005で使用する暗号アルゴリズムは、例えば、非特許文献1に記載のAES方式(128ビット鍵)などであり、実行装置12の実行部1217と同じ暗号アルゴリズムを用いる。ここでは暗号化コンテンツENCNTの生成方法として、各部分コンテンツに対して、全て同一のコンテンツ鍵CKで暗号化していたが、非特許文献1に記載のブロック暗号のモードを利用してよい。例えば、CBCモードやOFBモード、CFBモードなどでもよく、さらに、ある一定間隔毎にモード(例：CBCモード)の初期値を変化させるようにしたものでも良い。

【0045】

続いて、n個の暗号化部分コンテンツのそれぞれを識別、特定出来る、n個の特定情報ADDR#1、・・・、ADDR#nを取得する。このn個の特定情報は、例えば、暗号化コンテンツENCNTが複数のファイルから構成されている場合、各ファイルのファイル名である。ここでは、暗号化部分コンテンツENCNT#1を識別、特定する情報を特定情報ADDR#1、暗号化部分コンテンツENCNT#2を識別、特定する情報を特定情報ADDR#2、暗号化部分コンテンツENCNT#3を識別、特定する情報を特定情報ADDR#3、・・・、暗号化部分コンテンツENCNT#nを識別、特定する情報を特定情報ADDR#nとする。そして、暗号化コンテンツENCNTを可搬媒体イメージ生成部1007へ出力し、暗号化部分コンテンツと特定情報のn組{ENCNT#1、ADDR#1}、{ENCNT#2、ADDR#2}、・・・、{ENCNT#n、ADDR#n}を、ハッシュテーブル生成部1006へ出力する。

【0046】

なお、それぞれの特定情報は、上記で紹介した情報に限らず、各暗号化部分コンテンツを識別、特定出来るものであればどのような情報であっても良い。例えば、暗号化部分コンテンツの先頭の論理アドレスとサイズ(オフセット)、もしくは、先頭と終端の論理アドレス、もしくは、先頭の物理アドレスとサイズ(オフセット)、もしくは、先頭と終端の物理アドレス、などでもよい。

【0047】

(6) ハッシュテーブル生成部1006

ハッシュテーブル生成部1006は、暗号化部1005から、暗号化部分コンテンツと特定情報のn組{ENCNT#1、ADDR#1}、{ENCNT#2、ADDR#2}、・・・、{ENCNT#n、ADDR#n}とが入力された場合、以下のようにして、第一ハッシュテーブル群HASHTBL1G及び第二ハッシュテーブルHASHTBL2及びコンテンツ位置情報POSを生成する。

【0048】

n組の暗号化部分コンテンツと特定情報から第一ハッシュテーブル群HASHTBL1G及び第二ハッシュテーブルHASHTBL2及びコンテンツ位置情報POSを生成する大まかな流れは、図6で示す通りである。まず、n組の暗号化部分コンテンツと特定情報のそれぞれの組に対して、第一ハッシュテーブルHASHTBL1#1、HASHTBL1#2、・・・、HASHTBL1#nを生成する。そして、n個の第一ハッシュテーブルから構成される第一ハッシュテーブル群及び特定情報を用いて第二ハッシュテーブルHASHTBL2及びコンテンツ位置情報POSを生成する。

【0049】

まず、n組の暗号化部分コンテンツと特定情報のそれぞれの組に対して、第一ハッシュテーブルを生成する方法について説明する。ここでは例として、暗号化部分コンテンツENCNT#1と特定情報ADDR#1から第一ハッシュテーブルHASHTBL1#1

を生成する方法について説明する。なお、暗号化部分コンテンツE N C C N T # 2と特定情報A D D R # 2、・・・、E N C C N T # nと特定情報A D D R # nから第一ハッシュテーブルH A S H T B L 1 # 2、・・・、H A S H T B L 1 # nのそれぞれを生成する方法は、暗号化部分コンテンツE N C C N T # 1と特定情報A D D R # 1から第一ハッシュテーブルH A S H T B L 1 # 1を生成する方法と同じであるため、説明を省略する。まず、図7で示すように、暗号化部分コンテンツE N C C N T # 1をm個（mは1以上の自然数）のユニットU # 1、U # 2、・・・、U # mに分割する。分割する方法の一例としては、例えば暗号化部分コンテンツをある所定のサイズ毎に分割する方法がある。例えば、64キロバイト単位、1メガバイト単位、1秒単位、1分単位などである。ここで、暗号化部分コンテンツを所定のサイズ毎に分割した場合に余りのデータが出てしまう場合、余りとなった部分は一つのユニットとして扱わないようにする。なお、余りとなった部分に足りない部分がある所定の値（たとえば0など）で補充して、一つのユニットとして扱うようにしても良い。そして、m個のユニットのそれぞれを識別可能な第一識別子を生成する。第一識別子を生成する方法としては、例えば、各ユニットに自然数を順番に割り当てていく（1、2、・・・、m）方法などがある。ここで、各組に対して生成した第一識別子をそれぞれ、I D 1 # 1、I D 1 # 2、・・・I D 1 # mとし、次のように第一識別子とユニットが対応しているとする。{ I D 1 # 1、U # 1 }、{ I D 1 # 2、U # 2 }、・・・、{ I D 1 # m、U # n }。続いて、m組の第一識別子とユニットの各組に対して、ユニットの属性値（ハッシュ値）として第一ハッシュ値を計算する。ユニットの属性値である第一ハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献1に記載のSHA-1アルゴリズムやブロック暗号を用いたCBC-MACなどがあり、実行装置12の認証情報検証部1216で用いる方法と同じものを用いる。ここで、各組に対して計算した属性値たる第一ハッシュ値をそれぞれ、H A S H 1 # 1、H A S H 1 # 2、・・・、H A S H 1 # mとし、次のように第一識別子とユニットと第一ハッシュ値とが対応しているとする。{ I D 1 # 1、U # 1、H A S H 1 # 1 }、{ I D 1 # 2、U # 2、H A S H 1 # 2 }、・・・、{ I D 1 # m、U # m、H A S H 1 # m }。最後に、その中から第一識別子と第一ハッシュ値を抜き出し、第一ハッシュテーブルH A S H T B L # 1 = { I D 1 # 1、H A S H 1 # 1 }、{ I D 1 # 2、H A S H 1 # 2 }、・・・、{ I D 1 # m、H A S H 1 # m }を生成する。なお、暗号化部分コンテンツをm個のユニットに分割する方法は、上記の方法に限るものではない。例えば、コンテンツデータがD V D - V I D E O形式の動画コンテンツの場合、セル（C e l l）単位などでもよい。また、コンテンツデータがM P E G 2形式の動画コンテンツの場合、G O P単位、フィールド単位、フレーム単位、Iピクチャ単位などでもよい。コンテンツデータがディスクに記録されている場合、セクタ単位、論理セクタ単位、トラック単位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長（E C Cブロック単位）などでもよい。なお、第一識別子は、上記の方法によって生成されたものに限るものではない。例えば、各ユニットを識別可能な論理アドレスや物理アドレスでもよいし、乱数を用いてランダムな自然数を割り当ててもよい。

【0050】

続いて、n個の第一ハッシュテーブルと対応するn個の特定情報を用いて第二ハッシュテーブルH A S H T B L 2を生成する方法について、図8を用いて説明する。まず、n組の特定情報と第一ハッシュテーブルのそれぞれに対して、第一ハッシュテーブルの属性値（ハッシュ値）として第二ハッシュ値を計算する。第一ハッシュテーブルの第二ハッシュ値を求める方法としては、例えばm個の第一ハッシュ値と第一識別子の値を連結した値を一方向性関数に入力した場合の出力値を用いる方法があり、非特許文献1に記載のSHA-1アルゴリズムやブロック暗号を用いたCBC-MACなどがあり、実行装置12の認証情報検証部1216で用いる方法と同じものを用いる。ここで、各組に対して計算した第二ハッシュ値をそれぞれ、H A S H 2 # 1、H A S H 2 # 2、・・・、H A S H 2 # nとし、次のように特定情報と第一ハッシュテーブルと第二ハッシュ値が対応しているとする。{ A D D R # 1、H A S H T B L 1 # 1、H A S H 2 # 1 }、{ A D D R # 2、H A

SHTBL 1 # 2、HASH 2 # 2}、・・・、{ADDR # n、HASH TBL 1 # n、HASH 2 # n}。その中から特定情報と第二ハッシュ値とを抜き出し、第二ハッシュテーブルHASH TBL 2 = {ADDR # 1、HASH 2 # 1}、{ADDR # 2、HASH 2 # 2}、・・・、{ADDR # n、HASH 2 # n}を生成する。

【0051】

そして、n個の特定情報を用いてコンテンツ位置情報POSを生成する方法について説明する。まず、それぞれの特定情報ADDR # 1、ADDR # 2、・・・、ADDR # nに対して、対応する暗号化部分コンテンツを分割した際のユニットの個数であるユニット数をそれぞれNUMU # 1、NUMU # 2、・・・、NUMU # nとする。そして、図9で示すような、そのn組の特定情報とユニット数から構成される、コンテンツ位置情報POS = {ADDR # 1、NUMU # 1}、{ADDR # 2、NUMU # 2}、・・・、{ADDR # n、NUMU # n}を生成する。

【0052】

最後に、n個の第一ハッシュテーブルHASH TBL 1 # 1、HASH TBL 1 # 2、・・・、HASH TBL 1 # nから構成される第一ハッシュテーブル群HASH TBL 1 G及び第二ハッシュテーブルHASH TBL 2及びコンテンツ位置情報POSを、可搬媒体イメージ生成部1007へ出力する。そして、第二ハッシュテーブルHASH TBL 2及びコンテンツ位置情報POSを、認証情報生成部1010へ出力する。

【0053】

(7) 可搬媒体イメージ生成部1007

可搬媒体イメージ生成部1007は、暗号化鍵束生成部1004から暗号化鍵束KBとが入力され、ハッシュテーブル生成部1006から第一ハッシュテーブル群HASH TBL 1 G及び第二ハッシュテーブルHASH TBL 2及びコンテンツ位置情報POSとが入力され、暗号化部1005から暗号化コンテンツENCNTとが入力された場合、図10で示すような、可搬媒体11に記録するデータのイメージである可搬媒体イメージIMGを生成する。この可搬媒体イメージIMGは、例えば、可搬媒体11に記録した場合の物理アドレスを取得出来るものである。ここで、可搬媒体イメージIMGには、認証情報生成部1010で生成される認証情報AUTHを挿入するためにスペースを空けておくようにする。そして、その可搬媒体イメージIMGを配布データ領域特定情報生成部1008及び記録部1011へ出力する。

【0054】

(8) 配布データ領域特定情報生成部1008

配布データ領域特定情報生成部1008、可搬媒体イメージ生成部1007から可搬媒体イメージIMGとが入力された場合、可搬媒体11に記録するデータの領域を識別する配布データ領域特定情報AREAを取得、もしくは生成する。この配布データ領域特定情報AREAは、例えば、可搬媒体11に記録するデータの開始物理アドレスと最終物理アドレスの組である。もしくは、配布データ領域特定情報AREAは、例えば、可搬媒体11に記録するデータの最初物理アドレスと最終物理アドレスの組である。もしくは、配布データ領域特定情報AREAは、例えば、可搬媒体11に記録するデータの最初物理アドレスと最終物理アドレスの複数の組である。そして、その配布データ領域特定情報AREAを認証情報生成部1010及び記録部1011へ出力する。

【0055】

(9) 認証情報生成情報格納部1009

認証情報生成情報格納部1009は、第二ハッシュテーブル群HASH TBL 2 Gとコンテンツ位置情報POSと配布データ領域特定情報AREAの正当性を示す認証情報である認証情報AUTHを生成するための、認証情報生成情報GENAUTHが予め与えられ、保持するものである。この認証情報生成情報GENAUTHは、例えば、デジタル署名アルゴリズムの署名生成鍵(秘密鍵)である。認証情報生成情報GENAUTHに対応する検証情報VERは、実行装置12の検証情報格納部1215に格納されている。この検証情報VERは、例えば、デジタル署名アルゴリズムの署名検証鍵(公開鍵)である。デ

デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式やＲＳＡ署名などである。

【００５６】

（１０）認証情報生成部１０１０

認証情報生成部１０１０は、ハッシュテーブル生成部１００６から第二ハッシュテーブルHASH TBL ２及びコンテンツ位置情報POSとが入力され、配布データ領域特定情報生成部１００８から配布データ領域特定情報AREAとが入力された場合、以下のようにして、第二ハッシュテーブルHASH TBL ２及びコンテンツ位置情報POSと配布データ領域特定情報AREAを含む検証対象データに対する認証情報AUTHを生成する。まず、認証情報生成情報格納部１００９にアクセスして、認証情報生成情報GEN AUTHを取得する。そして、図１１で示すように、第二ハッシュテーブルHASH TBL ２及びコンテンツ位置情報POS及び配布データ領域特定情報AREAと認証情報生成情報GEN AUTHを用いて、認証情報AUTHを生成する。なお、認証情報AUTHの生成方法の一例は、デジタル署名アルゴリズムを用いる方法である。ここでは、デジタル署名アルゴリズムを用いる方法の一例を説明する。まず、第二ハッシュテーブルHASH TBL ２に含まれるｎ個の第二ハッシュ値とｎ個の特定情報と、コンテンツ位置情報POSに含まれるｎ個の特定情報とｎ個のユニット数から、第二ハッシュ値と特定情報とユニット数のｎ組を生成する。そして、それらの値と配布データ領域特定情報AREAの値を連結した値に対するデジタル署名を作成する。ここで、GENSIG（K、M）は署名生成鍵Kを用いてメッセージMに対して生成されたデジタル署名とすると、認証情報AUTHは、 $AUTH = GENSIG(GENAUTH, \{HASH2\#1 || ADDR\#1 || NUMU\#1\} || \{HASH2\#2 || ADDR\#2 || NUMU\#1\} || \dots || \{HASH2\#n || ADDR\#n || NUMU\#n\} || AREA)$ となる。そして、認証情報AUTHを記録部１０１１へ出力する。なお、認証情報生成部１０１０で使用するデジタル署名アルゴリズムは、実行装置１２の認証情報検証部１２１６で用いるデジタル署名アルゴリズムと同じものを用いる。

【００５７】

（１１）記録部１０１１

記録部１０１１は、配布データ領域特定情報生成部１００８から可搬媒体イメージIMGが入力され、認証情報生成部１０１０から認証情報AUTHが入力された場合、可搬媒体イメージIMGに予め確保されているデータ領域に認証情報AUTHを挿入して、図１２で示すような第二可搬媒体イメージIMG ２を生成する。そして、第二可搬媒体イメージIMG ２を可搬媒体１１へ記録する。例えば、可搬媒体１１は光ディスク（ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ）であり、記録部１０１１は与えられた第二可搬媒体イメージを基に光ディスクをプレス製造する機能を有する。なお、可搬媒体１１は書き込み可能光ディスク（ＣＤ－ＲやＤＶＤ－Ｒ、ＤＶＤ－ＲＡＭなど）であり、記録部１０１１は書き込み用レーザー等を用いて、与えられた第二可搬媒体イメージを基に光ディスクにデータを書き込む機能を有していてもよい。

【００５８】

<配布センタ１０の動作>

以上で、配布センタ１０の構成について説明を行ったが、ここでは配布センタ１０の動作の一例について、図１３に示すフローチャートの処理を行う。なお、配布センタ１０の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理にしても良い。

【００５９】

入力部１００１は、外部から入力されたコンテンツCNTを暗号化部１００５へ出力し、コンテンツ鍵生成要求REQをコンテンツ鍵生成部１００２へ出力する（ステップＳ１０１）。

コンテンツ鍵生成要求REQを入力されたコンテンツ鍵生成部１００２は、コンテンツ鍵CKを生成し、コンテンツ鍵CKを暗号化鍵束生成部１００４及び暗号化部１００５へ

出力する（ステップS102）。

【0060】

コンテンツ鍵CKを入力された暗号化鍵束生成部1004は、実行装置情報格納部1003にアクセスして複数の実行装置12が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵CKとを基に、暗号化鍵束KBを生成する。そして、暗号化鍵束KBを記録部1011に出力する（ステップ103）。

コンテンツCNT及びコンテンツ鍵CKが入力された暗号化部1005は、コンテンツ鍵CKを基に、コンテンツCNTを暗号化し、暗号化コンテンツENCNTを生成する。そして、暗号化コンテンツENCNTを可搬媒体イメージ生成部1007へ出力し、n組の暗号化部分コンテンツと特定情報を、ハッシュテーブル生成部1006へ出力する（ステップS104）。

【0061】

n組の暗号化部分コンテンツと特定情報を入力されたハッシュテーブル生成部1006は、n個の第一ハッシュテーブルHASHTBL1#1、・・・、HASHTBL1#nから構成される第一ハッシュテーブル群HASHTBL1G及び第二ハッシュテーブルHASHTBL2及びコンテンツ位置情報POSを生成する。そして、第一ハッシュテーブル群HASHTBL1G及び第二ハッシュテーブルHASHTBL2及びコンテンツ位置特定情報POSを可搬媒体イメージ生成部1007へ出力し、第二ハッシュテーブルHASHTBL2及びコンテンツ位置特定情報POSを認証情報生成部1010へ出力する（ステップS105）。

【0062】

可搬媒体イメージ生成部1007は、暗号化鍵束生成部1004から暗号化鍵束KBとが入力され、ハッシュテーブル生成部1006から第一ハッシュテーブル群HASHTBL1G及び第二ハッシュテーブルHASHTBL2及びコンテンツ位置情報POSとが入力され、暗号化部1005から暗号化コンテンツENCNTとが入力された場合、可搬媒体11に記録するデータのイメージである可搬媒体イメージIMGを生成する。そして、その可搬媒体イメージIMGを配布データ領域特定情報生成部1008及び記録部1011へ出力する。（ステップS106）

配布データ領域特定情報生成部1008は、可搬媒体イメージ生成部1007から可搬媒体イメージIMGとが入力された場合、可搬媒体11に記録するデータの領域を識別する配布データ領域特定情報AREAを取得、もしくは生成する。そして、その配布データ領域特定情報AREAを認証情報生成部1010及び記録部1011へ出力する。（ステップS107）

第二ハッシュテーブルHASHTBL2とコンテンツ位置情報POSと配布データ領域特定情報AREAを入力された認証情報生成部1010は、認証情報生成情報格納部1009にアクセスして、認証情報生成情報GENAUTHを取得する。そして、認証情報生成情報GENAUTHを用いて、第二ハッシュテーブルHASHTBL2とコンテンツ位置情報POSと配布データ領域特定情報AREAの正当性を示す認証情報である認証情報AUTHを生成する。そして、認証情報AUTHを記録部1011へ出力する（ステップS108）。

【0063】

記録部1011は、可搬媒体イメージ生成部1007から可搬媒体イメージIMGが入力され、認証情報生成部1010から認証情報AUTHが入力された場合、可搬媒体イメージIMGに認証情報AUTHを挿入して第二可搬媒体イメージIMG2を生成し、その第二可搬媒体イメージIMG2を可搬媒体11へ記録する。（ステップS109）

以上が、不正コンテンツ検知システム1の構成要素である配布センタ10の構成と動作である。続いて、可搬媒体11の構成について説明を行う。

【0064】

<可搬媒体11の構成>

可搬媒体11は、例えば、DVD-ROMやDVD-R、DVD-RAM、CD-ROM

M、C D－R等のような光ディスクの媒体（メディア）であり、図14に示すように、暗号化鍵束K Bと第一ハッシュテーブル群H A S H T B L 1 Gと第二ハッシュテーブルH A S H T B L 2とコンテンツ位置情報P O Sと配布データ領域特定情報A R E Aと認証情報A U T Hと暗号化コンテンツE N C C N Tとが配布センタ10によって記録されているものとする。

【0065】

以上が、不正コンテンツ検知システム1の構成要素である可搬媒体11の構成である。続いて、実行装置12の構成と動作について説明を行う。

＜実行装置12の構成＞

実行装置12は、図15に示すように、大きくドライブ部120とコンテンツ実行部121から構成される。ドライブ部120とコンテンツ実行部121は、例えば、バスなどにより接続されている。ドライブ部120は、読取部1201、配布データ領域特定情報格納部1202、第一秘密鍵格納部1203、第一秘匿通信処理部1204とから構成される。コンテンツ実行部121は、デバイス鍵格納部1211、コンテンツ鍵取得部1212、第二秘密鍵格納部1213、第二秘匿通信処理部1214、検証情報格納部1215、認証情報検証部1216、実行部1217とから構成される。

【0066】

（1）読取部1201

読取部1201は、可搬媒体11に記録されているデータの読み取りを行う。読取部1201は、実行装置12が可搬媒体11のデータを読み取り可能になった場合に、まず、可搬媒体11に記録されている配布データ領域特定情報A R E Aを取得し、配布データ領域特定情報格納部1202に格納する。そして、その配布データ領域特定情報A R E Aを第一秘匿通信処理部1204へ出力する。その後、可搬媒体11に記録されている暗号化鍵束K B及びコンテンツ位置情報P O S及び認証情報A U T Hを取得し、暗号化鍵束K Bをコンテンツ鍵取得部1212へ出力し、コンテンツ位置情報P O Sと認証情報A U T Hを認証情報検証部1216へ出力する。

【0067】

また、読取部1201は、認証情報検証部1216もしくは実行部1217から可搬媒体11に記録されているデータの読取要求が来た場合、まず配布データ領域特定情報格納部1202に格納されている配布データ領域特定情報A R E Aを取得する。そして、認証情報検証部1216もしくは実行部1217から読取要求が来たデータが配布データ領域特定情報A R E Aで識別される記録領域内であれば、可搬媒体11に記録されているデータ（第一ハッシュテーブル群H A S H T B L 1 G及び第二ハッシュテーブルH A S H T B L 2及び暗号化コンテンツE N C C N Tの全部、もしくは、一部）を取得して、読取要求が来た認証情報検証部1216もしくは実行部1217に出力する。例えば、配布データ領域特定情報A R E Aが可搬媒体11に記録されているデータの開始物理アドレスと最終物理アドレスを示している場合、読取要求が来たデータが配布データ領域特定情報A R E Aである開始物理アドレスよりも後の（大きい）アドレスにあり、かつ、最終物理アドレスよりも前の（小さい）アドレスにある場合、その該当データを認証情報検証部1216もしくは実行部1217に出力する。認証情報検証部1216もしくは実行部1217から読取要求が来たデータが配布データ領域特定情報A R E Aで識別される記録領域外であれば、読取要求が来た認証情報検証部1216もしくは実行部1217へはデータは出力しない。例えば、配布データ領域特定情報A R E Aが可搬媒体11に記録されているデータの開始物理アドレスと最終物理アドレスを示している場合、読取要求が来たデータが配布データ領域特定情報A R E Aである開始物理アドレスよりも前の（小さい）アドレスであるか、もしくは、最終物理アドレスよりも後の（大きい）アドレスにある場合、その該当データを認証情報検証部1216もしくは実行部1217へ出力しない。

【0068】

（2）配布データ領域特定情報格納部1202

配布データ領域特定情報格納部1202は、可搬媒体11に記録されている配布データ

領域特定情報A R E Aを保持するものである。配布データ領域特定情報A R E Aは、例えば、可搬媒体11に記録されているデータの開始物理アドレスと最終物理アドレスの組である。

【0069】

(3) 第一秘密鍵格納部1203

第一秘密鍵格納部1203は、第一秘匿通信処理部1204と第二秘匿通信処理部1214との間で秘匿通信を行うための鍵情報を保持するものであり、予め与えられる128ビットの鍵情報である共通秘密鍵S Kを保持する。与えられる共通秘密鍵S Kの値は、第二秘密鍵格納部1213が保持する共通秘密鍵S Kの値と同じである。なお、第一秘密鍵格納部1203は、共通秘密鍵S Kではなく、公開鍵暗号用の鍵情報（例えば、第一秘密鍵格納部1203の秘密鍵と第二秘密鍵格納部1213の公開鍵）を保持してもよい。

【0070】

(4) 第一秘匿通信処理部1204

第一秘匿通信処理部1204は、読取部1201から配布データ領域特定情報A R E Aが入力された場合、まず、第一秘密鍵格納部1203に格納されている共通秘密鍵S Kを取得する。そして、共通秘密鍵S Kを基に配布データ領域特定情報A R E Aの暗号化を行い、暗号化配布データ領域特定情報E N C A R E Aを生成する。そして、暗号化配布データ領域特定情報E N C A R E Aを第二秘匿通信処理部1214へ出力する。暗号アルゴリズムは、例えば、非特許文献1に記載のA E S方式（128ビット鍵）などであり、第二秘匿通信処理部1214と同じ暗号アルゴリズムを用いる。なお、例えば、非特許文献1に記載のチャレンジレスポンス認証方式を用いて、暗号化配布データ領域特定情報E N C A R E Aを第二秘匿通信処理部1214へ出力する前に、出力先である第二秘匿通信処理部1214の正当性を認証するようにしてもよい。また、例えば、非特許文献3に記載の鍵共有方法（Key Agreement Protocols）を用いて、第二秘匿通信処理部1214と毎回異なるセッション鍵S E Kを共有し、そのセッション鍵S E Kを基に、配布データ領域特定情報A R E Aを暗号化して、第二秘匿通信処理部1214へ出力してもよい。

【0071】

(5) デバイス鍵格納部1211

デバイス鍵格納部1211は、配布センタ10の実行装置情報格納部1003の中の鍵情報の一部を保持するものであり、デバイス鍵格納部1211に与えられる鍵情報と暗号化鍵束K Bを用いて、コンテンツ鍵C Kが取得出来るものである。例えば、実行装置情報格納部1003が図3のような場合、デバイス鍵格納部1211には、装置識別子A I D iとデバイス鍵K i（iは1からsのいずれか）が与えられる。

【0072】

(6) コンテンツ鍵取得部1212

コンテンツ鍵取得部1212は、読取部1201から暗号化鍵束K Bが入力された場合、デバイス鍵格納部1211に格納されている鍵情報及び暗号化鍵束K Bを用いて、コンテンツ鍵C Kを取得する。例えば、暗号化鍵束K Bが図4のような場合で、デバイス鍵格納部1211には装置識別子A I D iとデバイス鍵D K i（iは1からsのいずれか）が与えられている場合、コンテンツ鍵取得部1212はデバイス鍵格納部1211から装置識別子A I D iとデバイス鍵D K iを取得し、暗号化鍵束K Bの中から装置識別子A I D iに対応する暗号化コンテンツ鍵E N C C K i（E N C C K 1からE N C C K sの何れか）を取得する。そしてデバイス鍵D K iを基に、暗号化コンテンツ鍵E N C C K iを復号化することによって、コンテンツ鍵C K = D e c（D K i、E N C C K i）を取得する。なお、D e c（K、C）は暗号文Cを復号化鍵Kを用いて復号化した際の復号文とし、以後同じ意味で使用する。そして、コンテンツ鍵C Kを実行部1217へ出力する。

【0073】

(7) 第二秘密鍵格納部1213

第二秘密鍵格納部1213は、第二秘匿通信処理部1214と第一秘匿通信処理部12

04との間で秘匿通信を行うための鍵情報を保持するものであり、予め与えられる128ビットの鍵情報である共通秘密鍵SKを保持する。与えられる共通秘密鍵SKの値は、第一秘密鍵格納部1203が保持する共通秘密鍵SKの値と同じである。なお、第二秘密鍵格納部1213は、共通秘密鍵SKではなく、公開鍵暗号用の鍵情報（例えば、第二秘密鍵格納部1213の秘密鍵と第一秘密鍵格納部1203の公開鍵）を保持してもよい。

【0074】

（8）第二秘匿通信処理部1214

第二秘匿通信処理部1214は、第一秘匿通信処理部1214から暗号化配布データ領域特定情報ENCAREAが入力された場合、まず、第二秘密鍵格納部1213に格納されている共通秘密鍵SKを取得する。そして、共通秘密鍵SKを基に配布データ領域特定情報ARE Aの復号化を行い、配布データ領域特定情報ARE Aを生成する。そして、配布データ領域特定情報ARE Aを認証情報検証部1216へ出力する。暗号アルゴリズムは、例えば、非特許文献1に記載のAES方式（128ビット鍵）などであり、第一秘匿通信処理部1204と同じ暗号アルゴリズムを用いる。なお、例えば、非特許文献1に記載のチャレンジレスポンス認証方式を用いて、暗号化配布データ領域特定情報ENCARE Aを第一秘匿通信処理部1204から入力される前に、入力元である第一秘匿通信処理部1204の正当性を認証するようにしてもよい。また、例えば、非特許文献3に記載の鍵共有方法（Key Agreement Protocols）を用いて、第一秘匿通信処理部1204と毎回異なるセッション鍵SEKを共有し、そのセッション鍵SEKを基に、暗号化配布データ領域特定情報ENCARE Aを復号化して、認証情報検証部1216へ出力してもよい。

【0075】

（9）検証情報格納部1215

検証情報格納部1215は、認証情報AUTHの正当性を検証するために必要な検証情報VERを保持するものである。この検証情報VERに対応する認証情報生成情報GENAUTHは、配布センタ10の認証情報生成情報格納部1009に格納されている。例えば、検証情報VERはデジタル署名アルゴリズムの署名検証鍵（公開鍵）である。

【0076】

（10）認証情報検証部1216

認証情報検証部1216は、読取部1201からコンテンツ位置情報POS及び認証情報AUTHが入力され、第二秘匿通信処理部1214から配布データ領域特定情報ARE Aが入力された場合、認証情報AUTHの正当性を検証する。検証は以下のように行われる。

【0077】

まず、図16で一例を示すように、コンテンツ位置情報POSに含まれるn組の特定情報ADDR#1、・・・、ADDR#nとユニット数NUMU#1、・・・、NUMU#nから、i組（iは1以上n-1以下の自然数）の特定情報とユニット数を選択する。ここで、選択されたi組の特定情報とユニット数からなるデータを被選択コンテンツ位置情報とする。ここでは、第三者によってどの特定情報とユニット数が選択されるか推測できないようにする。この方法は、例えば真性乱数や擬似乱数を用いることにより実現出来る。真性乱数は、例えばノイズなどを利用することにより発生出来る。擬似乱数は、例えば擬似乱数生成アルゴリズムとシードを用いることにより発生出来る。これらは共に、認証情報検証部1216が乱数生成器を有することにより実現出来る。これら乱数を生成する方法については、非特許文献2が詳しい。なお、乱数生成器を利用しなくても、推測出来ない情報であれば何でも良い。例えば、気温や湿度などでも良い。これは、認証情報検証部1216が温度センサや湿度センサを有することにより実現出来る。

【0078】

続いて、図17で示すように、選択されたi組の特定情報とユニット数（被選択コンテンツ位置情報）、及び、可搬媒体11に記録されている第二ハッシュテーブルHASH TBL2の一部を基に、入替第二ハッシュテーブルREPHASHTBL2を生成する。入

替第二ハッシュテーブル REPHASHTBL 2 を生成する方法は、以下の通りである。まず、選択された i 組の特定情報とユニット数のそれぞれに対応する i 個の入替第一ハッシュテーブルを生成する。ここでは、選択された i 組の特定情報とユニット数のうち、1 組が特定情報 ADDR # 1 とユニット数 NUMU # 1 である場合を例に挙げ、入替第一ハッシュテーブル REPHASHTBL 1 # 1 を生成する手順について説明する。なお、他の特定情報とユニット数の場合であっても、同様の手順となる。まず、ユニット数 NUMU # 1 を基に、特定情報 ADDR # 1 に対応する暗号化部分コンテンツ ENCCNT # 1 に含まれるユニットの数を認識し、1 番目から d 番目（d はユニット数 NUMU # 1）までのユニットのうち、j 個（j は 1 以上 m 以下の自然数）のユニットを選択する。ここでも、第三者によってどのユニットが選択されるか推測できないようにする。この方法は、先ほど、コンテンツ位置情報 POS に含まれる n 組の特定情報とユニット数から、i 組の特定情報とユニット数を選択する方法と同様の方法が利用可能であるため、説明を省略する。以後、説明を簡略化するために、j は 1 とし、図 18 で示すように、ユニット U # 3（図 18 における横点線）が選択されたとする。そして、そのユニット U # 3 に対する属性値である第一ハッシュ値 H 1（図 18 における縦線）を計算する。また、特定情報 ADDR # 1 及びユニット数 NUMU # 3 を基に、読取部 1201 経由で可搬媒体 11 から ID 1 # 3 以外の選択されなかった第一識別子に対応する第一ハッシュ（図 18 における横点線）を取得する。そして、選択された第一識別子に対応するユニットの属性値を計算することによって取得した第一ハッシュ値、及び、選択されなかった第一識別子に対応する第一ハッシュ値から構成される、図 18 で示される、入替第一ハッシュテーブル REPHASHTBL 1 # 1 を生成する。

【0079】

続いて、生成された i 個の入替第一ハッシュテーブル、及び、可搬媒体 11 に記録されている第二ハッシュテーブル HASHTBL 2 の一部を基に、入替第二ハッシュテーブル REPHASHTBL 2 を生成する方法について説明する。図 19 で一例を示すように、まず、i 個の入替第一ハッシュテーブルのそれぞれに対する属性値として、第二ハッシュ値（図 19 における縦線）を生成する。図 19 では、入替第一ハッシュテーブル REPHASHTBL 1 # 1 に対する属性値として第二ハッシュ値 H 2 # 1、・・・、入替第一ハッシュテーブル REPHASHTBL 1 # c に対する属性値として第二ハッシュ値 H 2 # c としている。次に、選択されなかった特定情報に対応する第二ハッシュ値を、読取部 1201 経由で可搬媒体 11 から取得する（図 19 における横点線）。そして、入替第一ハッシュテーブルの属性値を計算することによって取得した第二ハッシュ値、及び、選択されなかった特定情報に対応する第二ハッシュ値から構成される、図 19 で示される、入替第二ハッシュテーブル REPHASHTBL 2 を生成する。

【0080】

最後に、検証情報格納部 1215 に格納されている検証情報 VER を使って、図 20 で示すように、認証情報 AUTH が発行センタ 10 による入替第二ハッシュテーブル REPHASHTBL 2 及びコンテンツ位置情報 POS 及び配布データ領域特定情報 AREA に対する正規の認証情報であるかを検証する。例えば、まず、入替第二ハッシュテーブル REPHASHTBL 2 に含まれる n 個の第二ハッシュ値と n 個の特定情報と、コンテンツ位置情報 POS に含まれる n 個の特定情報と n 個のユニット数から、第二ハッシュ値と特定情報とユニット数の n 組を生成し、デジタル署名検証アルゴリズムを用いて、認証情報 AUTH がそれらの値と配布データ領域特定情報 AREA を結合した値 {HASH 2 # 1 || ADDR # 1 || NUMU # 1} || {HASH 2 # 2 || ADDR # 2 || NUMU # 1} || ... || {HASH 2 # n || ADDR # n || NUMU # n} || AREA に対する正規のデジタル署名であるかどうか検証する。このデジタル署名検証アルゴリズムは、配布センタ 10 の認証情報生成部 1010 で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。なお、デジタル署名アルゴリズムは、例えば、非特許文献 1 に記載の DSA 方式などである。認証情報検証部 1216 は、認証情報 AUTH が発行センタ 10 による正しい認証情報である場合にのみ、実行開始許可情報

P E R Mを実行部 1 2 1 7 へ出力する。なお、被選択コンテンツ位置情報に含まれる i 個の特定情報に対応する i 個の暗号化部分コンテンツを、被選択部分コンテンツとする。なお、コンテンツ位置情報 P O S に含まれる n 組の特定情報 A D D R # 1、・・・、A D D R # n とユニット数 N U M U # 1、・・・、N U M U # n から、 i 組の特定情報とユニット数を選択する際、同じ特定情報とユニット数の組を重複して選択するようにしてもよい。なお、選択した i 組の特定情報とユニット数の各組に対して、それぞれ異なるユニットの数 (j) を選択するようにしてもよい。

【 0 0 8 1 】

(1 1) 実行部 1 2 1 7

実行部 1 2 1 7 は、コンテンツ鍵取得部 1 2 1 2 からコンテンツ鍵 C K が入力され、かつ、認証情報検証部 1 2 1 6 から実行開始許可情報 P E R M が入力された場合に、読取部 1 2 0 1 経由で、可搬媒体 1 1 に記録されている暗号化コンテンツ E N C C N T を逐次取得し、逐次コンテンツ鍵 C K を基に復号化を行って、逐次実行するものである。例えば、実行部 1 2 1 7 は M P E G 2 データや M P 3 データをデコードする機能を有するデコータを有していて、M P E G 2 形式の動画コンテンツや M P 3 形式の音声コンテンツであるコンテンツ C N T を逐次デコードして、外部に出力するものである。また、例えば、実行部 1 2 1 7 は、ディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生するようなものでも良いし、別の可搬媒体や記録媒体にコンテンツデータを出力するようなものでも良いし、印刷機能を有しコンテンツデータを紙などに印刷するようなものでもよい。

【 0 0 8 2 】

< 実行装置 1 2 の動作 >

以上で、実行装置 1 2 の構成について説明を行ったが、ここで実行装置 1 2 の動作について、図 2 1 に示すフローチャートを用いて説明する。なお、実行装置 1 2 の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理しても良い。

【 0 0 8 3 】

実行装置 1 2 が可搬媒体 1 1 のデータを読み取り可能になった場合に、読取部 1 2 0 1 は可搬媒体 1 1 に記録されている配布データ領域特定情報 A R E A を取得し、配布データ領域特定情報 A R E A を配布データ領域特定情報格納部 1 2 0 2 に格納する。そして、配布データ領域特定情報 A R E A を第一秘匿通信処理部 1 2 0 4 へ出力する。(ステップ S 1 2 1)

読取部 1 2 0 1 は可搬媒体 1 1 に記録されている暗号化鍵束 K B 及びコンテンツ位置情報 P O S 及び認証情報 A U T H を取得し、暗号化鍵束 K B をコンテンツ鍵取得部 1 2 1 2 へ出力し、コンテンツ位置情報 P O S と認証情報 A U T H を認証情報検証部 1 2 1 6 へ出力する。(ステップ S 1 2 2)。

【 0 0 8 4 】

配布データ領域特定情報 A R E A が入力された第一秘匿通信処理部 1 2 0 4 は、第一秘密鍵格納部 1 2 0 5 が保持する秘密共有鍵 S K を基に配布データ領域特定情報 A R E A を暗号化し、暗号化配布データ領域特定情報 E N C A R E A を取得し、暗号化配布データ領域特定情報 E N C A R E A を第二秘匿通信処理部 1 2 1 4 へ出力する。(ステップ S 1 2 3)

暗号化鍵束 K B を入力されたコンテンツ鍵取得部 1 2 1 2 は、デバイス鍵格納部 1 2 1 1 が保持している鍵情報を用いて、コンテンツ鍵 C K を取得する。そして、コンテンツ鍵 C K を実行部 1 2 1 7 へ出力する。(ステップ S 1 2 4)

暗号化配布データ領域特定情報 E N C A R E A が入力された第二秘匿通信処理部 1 2 1 4 は、第二秘密鍵格納部 1 2 1 5 が保持する秘密共有鍵 S K を基に暗号化配布データ領域特定情報 E N C A R E A を復号化し、配布データ領域特定情報 A R E A を取得し、配布データ領域特定情報 A R E A を認証情報検証部 1 2 1 6 へ出力する。(ステップ S 1 2 5)

コンテンツ位置情報 P O S と配布データ領域特定情報 A R E A と認証情報 A U T H を入

力された認証情報検証部1216は、コンテンツ位置情報POSを基に、可搬媒体11に記録されている第一ハッシュテーブル群HASH_TBL1G及び第二ハッシュテーブルHASH_TBL2の一部を用いて入替第二ハッシュテーブルREPHASH_TBL2を生成する。(ステップS126)

認証情報検証部1216は、検証情報格納部1215に格納されている検証情報VERを使って、認証情報AUTHが発行センタ10によるコンテンツ位置情報POSと配布データ領域特定情報AREAと入替第二ハッシュテーブルREPHASH_TBL2の認証情報であるかを検証する。(ステップS127)

認証情報検証部1216は、認証情報AUTHが発行センタ10による正しい認証情報である場合にのみ、実行開始許可情報PERMを実行部1217へ出力し、ステップS129へ進む。もし、認証情報AUTHが正しい認証情報ではない場合、処理を終了する。(ステップS128)

コンテンツ鍵CK及び実行開始許可情報PERMを入力された実行部1217は、読取部1201経由で、可搬媒体11に記録されている暗号化コンテンツENC_CNTを逐次取得し、逐次コンテンツ鍵CKを基に復号化を行って、逐次実行する。ここで、実行部1217から可搬媒体11に記録されているデータの読取要求が来た読取部1201は、配布データ領域特定情報格納部1202に格納されている配布データ領域特定情報AREAを取得し、実行部1217から読取要求が来たデータが配布データ領域特定情報AREAで識別される記録領域内であれば、可搬媒体11に記録されているデータを取得して、実行部1217に出力するようにする。(ステップS129)

以上が、不正コンテンツ検知システム1の構成要素である実行装置12の構成と動作である。尚、配布データ領域特定情報格納部1202、第一秘密鍵格納部1203、第一秘匿通信処理部1204、等の各機能ブロックは典型的には集積回路であるLSIとして実現されていてもよい。同様に、デバイス鍵格納部1211、コンテンツ鍵取得部1212、第二秘密鍵格納部1213、第二秘匿通信処理部1214、検証情報格納部1215、認証情報検証部1216、実行部1217等の各機能ブロックは典型的には集積回路であるLSIとして実現されていてもよい。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

【0085】

ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用して良い。

【0086】

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

＜不正コンテンツ検知システム1の効果＞

以上、不正コンテンツ検知システム1について実施の形態に基づいて説明したが、この不正コンテンツ検知システム1においては、配布センタ10は、著作権者によって可搬媒体11に記録されたデータのデータ領域の領域である配布データ領域特定情報AREAを記録するようにして、実行装置12では、その配布データ領域特定情報AREAで指定されたデータ領域の領域外にあるデータは取得しないようにした。実施の形態において、配布データ領域特定情報は、可搬媒体11に記録されているデータの開始物理アドレスと最終物理アドレスの組である。このことにより、実行装置12では配布データ領域特定情報AREAにより予め著作権者によって指定された領域外のデータは取得しないため、不正コンテンツを実行、再生出来ないようになる。また可搬媒体11には、さらに、配布データ領域特定情報AREAに対する認証情報AUTHを記録するようにして、実行装置12

では、認証情報AUTHが可搬媒体11に記録された配布データ領域特定情報AREAに対する正規の著作権者の認証情報であるか検証し、検証が成功した場合にのみ、コンテンツの実行、再生を行うようにした。このことにより、著作権を保持しない不正者が、可搬媒体11の記録されている配布データ領域特定情報AREAを改ざんしたとしても、その可搬媒体11に記録されているコンテンツは実行、再生しないようになった。このことにより、上記で示したような不正行為に対する耐性を向上させることが出来る。

【0087】

また、実行装置12において、配布された不正コンテンツが実行、再生される不正行為の別の形態として、可搬媒体11に記録されているデータを読み出すドライブ部120と、ドライブ部120によって取得されたデータを実行、再生するコンテンツ実行部121との間に流れるデータを改竄される場合がある。そこで、ドライブ部120からコンテンツ実行部121へ出力するデータの一部（例えば、配布データ領域特定情報AREA）を暗号化して出力するようにした。これにより、不正者は、ドライブ部120が出力したデータを別のデータに差し替えてコンテンツ実行部121へ出力しようとしても、不正者は正しく暗号化することが出来ないため、正しくコンテンツ実行部121へ出力できなくなった。この際、同じデータであっても、ドライブ部からコンテンツ実行部へ出力する暗号文が異なるようにしてもよい。これは、例えば、ドライブ部120とコンテンツ実行部121が毎回異なるセッション鍵を共有することにより実現出来る。このことにより、著作権を保持しない不正者によって不正コンテンツが実行、再生されるという不正行為を防ぐことが出来るようになった。

<変形例>

上記に説明した実施の形態は、本発明の実施の形態の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

【0088】

（1）本発明は、上記に示す実行装置12のコンテンツ実行部121の動作を、図22で例を示すようなドライブ部を有するコンピュータにより実現するコンピュータプログラムであるとしてもよい。さらには、前記コンピュータプログラムからなるデジタル信号であるとしても良い。

（2）上記で説明した実施の形態は、本発明の不正コンテンツ検知システムの一実施形態にすぎない。本発明の効果をを得るために、以下の動作のみで十分であることを補足しておく。まず、配布センタ10は、実行装置12へ配布するコンテンツCNTの領域を特定する配布データ領域特定情報AREA（例えば、開始物理アドレスと最終物理アドレスの組）を生成し、その配布データ領域特定情報AREAを含む検証対象データに対する認証情報AUTHを生成し、コンテンツCNTと配布データ領域特定情報AREAと認証情報AUTHを実行装置12へ配布する。実行装置12は、配布データ領域特定情報を基に認証情報を検証し、検証結果が正当な場合にのみ、配布データ領域特定情報を基に配布データを特定し、その配布データのみをコンテンツとして実行、もしくは再生する。これにより、本発明の効果は得ることが出来る。

【0089】

（3）実施の形態1では、不正者によってドライブ部120が出力したデータを別のデータに差し替えて正しくコンテンツ実行部121へ出力出来ないようにすることを目的に、配布データ領域特定情報AREAだけを暗号化していたが、これに限るものではない。例えば、ドライブ部120がコンテンツ実行部121へ出力するデータを全て暗号化するようにしてもよい。もしくは、ドライブ部120がコンテンツ実行部121へ出力する配布データ領域特定情報AREA以外のデータ（例えば、暗号化鍵束、第一ハッシュテーブル群、第二ハッシュテーブル、コンテンツ位置情報、認証情報、暗号化コンテンツの全部もしくは一部のデータ）を暗号化するようにしてもよい。もしくは、ドライブ部120がコンテンツ実行部121へ出力するデータを全く暗号化しないようにしてもよい。

【0090】

(4) 実施の形態1の可搬媒体11に記録されている配布データ領域特定情報AREAは、可搬媒体11に記録されているデータの領域を識別するものだけに限るものではない。一例として、例えば、配布データ領域特定情報AREAは、可搬媒体11に記録されているデータの最終物理アドレスだけでもよい。もしくは、可搬媒体11に記録されているデータの開始物理アドレスだけでもよい。もしくは、可搬媒体11に記録されているデータの総サイズであってもよい。例えば、配布センタ10は、可搬媒体11に記録するデータの総サイズを配布データ領域特定情報AREAとして生成し、その配布データ領域特定情報AREAを可搬媒体11に記録する。そして、実行装置12の読取部1201では、可搬媒体11に記録された配布データ領域特定情報AREAを取得する。その後、読取部1201は、可搬媒体11から取得したデータの総サイズを計測する。そして、読取部1201は、可搬媒体11から取得したデータの総サイズが、可搬媒体11に記録された配布データ領域特定情報AREAで識別されるサイズよりも多くなった場合、以後読取部1201は、可搬媒体11からデータを取得しないようにする。これにより、著作権を保持しない不正者により、新たな可搬媒体に、正規の配布センタによって配布された可搬媒体のデータをそのまま記録して、新たな可搬媒体においてまだ記録可能な領域に不正コンテンツを記録された場合でも、読取部1201は予め著作権者によって指定されたデータの総サイズ以上は取得しないため、そのような不正行為を防止することが出来る。

【0091】

(5) 実施の形態1の配布センタ10は、図2で示すような構成に限るものではない。例えば、図23で示すように、認証情報AUTHを生成する認証情報生成部1010は発行センタが行うようにしても良い。この場合、発行センタは、例えば、正規の著作権者であり、可搬媒体11へ記録するのは、例えば、ディスク製造業者（プレス業者）などである。

【0092】

(6) 実施の形態1のコンテンツCNTは、動画データや音声データなどのコンテンツであったが、これに限るものではない。例えば、コンテンツは画像コンテンツでもよいし、テキストコンテンツでもよい。また、コンピュータプログラムであっても良い。この場合、実行装置12は、コンピュータプログラムを実行するために必要なCPUやメモリ、ディスクなどを備えていれば良い。こうすることにより、実行装置12では、不正なコンピュータプログラムを実行開始しないようになるため、コンピュータウイルス等を防ぐ対策として有効となる。

【0093】

(7) 実施の形態1において、可搬媒体11に記録されるデータは、図14のような順番で記録されていなくてもよい。

(8) 実施の形態1において、可搬媒体11には、暗号化コンテンツENC CNT以外の第二コンテンツCNT2を記録するようにしても良い。そして、暗号化コンテンツENC CNTの検証処理を行っている間に、その第二コンテンツCNT2を実行、再生するようにしてもよい。例えば、その第二コンテンツCNT2の例としては、映画のオープニング画面やDVDのメニュー画面、違法コピーに関する警告文書、コンテンツ配給者のロゴやオープニング画面などが挙げられる。なお、第二コンテンツCNT2は、予め実行装置12内に格納されていても良い。

【0094】

(9) 実施の形態1において、可搬媒体11に記録されている暗号化コンテンツENC CNTの検証処理を行っている間に、配布センタ10によって許諾された暗号化コンテンツENC CNTのある一部分を実行、再生するようにしてもよい。例えば、その暗号化コンテンツENC CNTのある一部分の例としては、映画のオープニング画面やDVDのメニュー画面、違法コピーに関する警告文書、コンテンツ配給者のロゴやオープニング画面などが挙げられる。

【0095】

(10) 実施の形態1において、暗号化部分コンテンツの属性値(ハッシュ値)は2層構造であってが、これに限るものではない。例えば、暗号化部分コンテンツの属性値(ハッシュ値)の集合を第一ハッシュテーブルとして、認証情報AUTHはその第一ハッシュテーブルに対する認証情報としてもよい(1層型)。もしくは、暗号化部分コンテンツの属性値(ハッシュ値)の集合を第一ハッシュテーブルとして、第一ハッシュテーブルをグループ分けし、その各グループの第一ハッシュテーブルを連結した値に対する属性値(ハッシュ値)を第二ハッシュテーブルとして、第二ハッシュ値をグループ分けし、その各グループの第二ハッシュ値を連結した値に対する属性値(ハッシュ値)を第三ハッシュテーブルとして、認証情報AUTHはその第三ハッシュテーブルに対する認証情報としてもよい(3層型)。もしくは、4層以上の構造にしてもよい。層を深くすることにより、可搬媒体に記録すべき属性値の数は増えるが、実行装置が可搬媒体から取得すべき属性値の数を減らすことが出来る。一方、層を浅くすることにより、実行装置が可搬媒体から取得すべき属性値の数は増えるが、可搬媒体に記録すべき属性値の数を減らすことが出来る。このようにバランスを変えることが出来るようになる。

【0096】

(11) 実施の形態1の可搬媒体11において、図24で示すように、n個の暗号化部分コンテンツの再生、実行手順を記述したデータである実行手順データNAVを記録するようにして、実行装置12の実行部1217では、その実行手順データNAVを基に、n個の暗号化部分コンテンツを再生、実行するようにしてもよい。この場合、配布センタ10は、その実行手順データNAVを含めたデータに対する認証情報を生成するようにして、実行装置12では、認証情報によりその実行手順データNAVの正当性が検証された場合にのみ、実行部1217へ暗号化コンテンツENCNTを実行、再生するようにしてもよい。なお、実行手順データNAVは、例えば、DVD-VIDEO形式におけるナビゲーションファイル(拡張子がIFOのファイル)である。

【0097】

(12) 実施の形態1において、コンテンツCNTは予めn個の部分コンテンツに分割されているとしたが、これに限るものではない。例えば、コンテンツCNTが予めn個の部分コンテンツに分割されていない場合、入力部1001は、ある所定の区切りに従ってコンテンツCNTをn個に分割するようにしても良い。この所定の区切りは、予めシステム共通のパラメータとして与えられていても良いし、外部から入力されてもよい。外部から入力される場合、例えば、入力部1001がキーボードやマウスと接続されていることにより実現できる。所定の区切りは、例えば、64キロバイト単位、1メガバイト単位、1秒単位、1分単位でもよい。また、別の例として、コンテンツデータがDVD-VIDEO形式の動画コンテンツの場合、VOB単位や、VOBU(Video Object Unit)単位、セル(Cell)単位などでもよい。コンテンツデータがMPEG2形式の動画コンテンツの場合、例えば、GOP単位、フィールド単位、フレーム単位、Iピクチャ単位などでもよい。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、論理セクタ単位、トラック単位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長(ECCブロック単位)などでもよい。なお、部分コンテンツのサイズは、全て同じである必要はなく、それぞれ異なってもよい。また、コンテンツを分割する数(n)は、コンテンツCNTに応じて変えても良い。

【0098】

(13) 実施の形態1において、実行装置12の読取部1201は、可搬媒体11から複数のユニットを取得する場合、アクセス時間の高速化を目的に、ユニットを取得する順番を最適化するようにしても良い。

ここでは一例として、以下のような状況を想定する。実行装置12の読取部1201は、4個のユニットU#1、U#2、U#3、U#4を取得したいとする。また、可搬媒体11は、CD-ROMやDVD-ROMなどの光ディスクであるとする。その可搬媒体11(光ディスク)上には、データを記録する部分があくつかに分かれており、年輪状に広がっている各領域をトラックと呼ぶ。各トラックには、いくつかのセクタを含み、データ

はセクタ単位で読み書きされる。例えば、1セクタのサイズは512バイトである。このような場合、可搬媒体11上の読み取り対象データは、トラック識別番号やセクタ識別番号やセクタサイズにより特定することが出来る。読取部1201は、ヘッド機構部（ピックアップ）及び回転軸を備え、回転軸により可搬媒体11（光ディスク）を半時計回りに回転させるものとする。ヘッド機構部（ピックアップ）から特定情報（トラック識別番号やセクタ識別番号やセクタサイズ）を指定することで、対象部分のデータを取得出来るものとする。ここでは、4個のユニットU#1、U#2、U#3、U#4は、図25のように可搬媒体11（光ディスク）上の位置に記録されているとし、可搬媒体11（光ディスク）とヘッド機構部も、図25で示す場所に存在しているとする。ここで、一般に、該当読取位置に対応するトラック位置へヘッド機構部（ピックアップ）を移動させる時間がかかることが知られている。言い換えると、可搬媒体11（光ディスク）上における内周のトラックから外周方向への移動、もしくは、外周のトラックから内周方向への移動に大きな処理時間がかかることに起因している。可搬媒体11（光ディスク）上における内側のトラック上にあるデータを読み込んだ後に、外側のトラック上にあるデータを読み込み、その後、また内側のトラック上にあるデータを読み込む場合がその一例である。

【0099】

上記のような状況の場合、実施の形態1の動作に沿えば、まず1番目に、ユニットU#1の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。その後、2番目にユニットU#2の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。その後も同様に、ユニットU#3の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得し、最後に、ユニットU#4の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。つまり、ユニットU#1を取得するまでに、ヘッド機構部を内周から外周へ移動させ、続いて、ユニットU#2を取得するまでに、ヘッド機構部を外周から内周へ移動させる。その後も、ユニットU#3を取得するまでに、ヘッド機構部を内周から外周へ移動させ、最後に、ユニットU#4を取得するまでに、ヘッド機構部を外周から内周へ移動させる。つまり、4つのデータを取得するまでに、ヘッド機構部を何度も移動往復させる必要があることが分かる。

【0100】

そこで、本変形例では、上記全4つのデータの取得時間を短くする目的で、実行装置12の読取1201は、まずはじめに、それぞれのデータを取得する順序の最適値を計算する。例えば、一番初めに一番内側のトラック上にあるデータを全て取得して、その次に、一つ外側のトラック上にあるデータを全て取得いく、というようなことを繰り返す。この場合、トラック上に一つもデータがない場合は、そのトラックをスキップして次のトラックに進むようにする。例えば、4つのユニットが図25のように可搬媒体11（光ディスク）上の位置に記録されているとし、さらに、可搬媒体11（光ディスク）及びヘッド機構部（ピックアップ）が図25で示す場所に存在しているとする。すると、このデータを取得する順序の最適値は、内周側から外周側に向かって、ユニットU#2、ユニットU#4、ユニットU#3、ユニットU#1となる。このようにすることで、可搬媒体11（光ディスク）上に記録されているとびとびの部分データをランダムに取得する（いわゆるランダムアクセス）場合にでも、取得したい全てのデータを取得するまでの時間を短縮することが出来る。なお、当然、ユニットは4個以外であっても適用可能である。

【0101】

なお、最適化手段は、読取部1201（ヘッド機構部や回転軸等）の動作の特徴に依存するため、本変形例で説明した最適化手段は、あくまで一例であることを注意しておく。例えば、光ディスクの回転制御方式には、角速度一定方式や線速度一定方式があり、これらの特徴を考慮するようにしても良い。また、可搬媒体11は当然光ディスクでなくてもよく、例えばハードディスクなどでも同様のことが実現出来る。

【0102】

（14）実施の形態1において、認証情報検証部1216は、予め与えられているパラ

メータ i 、 j に従って検証を実施していたが、これに限るものではない。例えば、配信装置 10 は可搬媒体 11 に、パラメータ i 、 j の両方もしくは片方を記録するようにして、実行装置 12 は可搬媒体 11 に記録されているパラメータ i 、 j の両方もしくは片方に従って検証するようにしてもよい。この場合、配布センタ 10 は、そのパラメータ i 、 j の両方（もしくは片方）を含めたデータに対する認証情報を生成するようにして、実行装置 12 では、認証情報によりそのパラメータ i 、 j の両方（もしくは片方）の正当性が検証された場合にのみ、実行部 1217 へ暗号化コンテンツ $ENCNT$ を実行、再生するようにしてもよい。このパラメータ i 、 j は、多くすればセキュリティは向上するが、処理時間が多くなり、少なくすれば処理時間は少なくなるが、セキュリティは低下するという特徴を有する。つまり、本変形例を用いることで、著作権者（コンテンツ配布者）の要望やポリシーに依存して、セキュリティレベルなどを設定することが出来るようになる。なお、実行装置 12 において、可搬媒体 11 にパラメータ i 、 j が記録されていない場合、予め与えられるデフォルトのパラメータ i 、 j を用いるようにしても良い。

【0103】

(15) 実施の形態 1 において、コンテンツ位置情報 POS は、 n 個の暗号化部分コンテンツの構成、及び、暗号化部分コンテンツの中のユニットの構成を特定出来るものであれば、どのようなものでもよい。例えば、特定情報は、暗号化部分コンテンツを識別する光ディスク上の先頭の論理アドレスとオフセット（データサイズ）でもよい。もしくは、先頭の論理アドレスと終端の論理アドレスであっても良い。もしくは、先頭の物理アドレスとオフセット（データサイズ）であっても良い。もしくは、先頭の物理アドレスと終端の物理アドレスであっても良い。さらに、ユニット数は、各ユニットの先頭の論理アドレスとデータサイズの羅列であってもよい。もしくは、先頭と終端の論理アドレスの羅列であってもよい。もしくは、先頭の物理アドレスとデータサイズの羅列であってもよい。もしくは、先頭と終端の物理アドレスの羅列であっても良い。

【0104】

また、コンテンツ位置情報 POS において、各特定情報に対応する暗号化部分コンテンツに含まれるユニット数が同じ場合、図 26 で示すとおり、 n 個のユニット数の替わりに 1 つの共通ユニット数 $ALLNUMU$ （一つの第二ハッシュ値が、いくつの第一ハッシュ値から計算されているかを示す属性値比率）がコンテンツ位置情報 POS に含まれていても良い。この場合、認証情報 $AUTH$ は、図 27 で示すように、第二ハッシュテーブル $HASHTBL2$ 及び共通ユニット数 $ALLNUMU$ を連結した値に対する認証情報として、実行装置 12 における検証時には、図 28 で示すように、認証情報 $AUTH$ が入替第二ハッシュテーブル $REPHASHTBL2$ 及び共通ユニット数 $ALLNUMU$ を連結した値に対する正しい認証情報であるか検証するようにしても良い。

【0105】

(16) 実施の形態 1 の認証情報 $AUTH$ は、第二ハッシュテーブル $HASHTBL2$ とコンテンツ位置情報 POS と配布データ領域特定情報 $AREA$ とを連結した値に対する認証情報であったが、これに限るものではない。例えば、第二ハッシュテーブル $HASHTBL2$ とコンテンツ位置情報 POS と配布データ領域特定情報 $AREA$ に加え、コンテンツ鍵 CK を連結した値に対する認証情報であっても良い。こうすることにより、コンテンツ鍵 CK を持たないものは、認証情報 $AUTH$ の正当性を検証出来なくなり、安全性がより高まる。また、例えば、第二ハッシュテーブル $HASHTBL2$ に含まれる n 個の第二ハッシュ値とコンテンツ位置情報 POS に含まれる n 個の特定情報と n 個のユニット数と配布データ領域特定情報 $AREA$ を連結した値に対する認証情報であっても良い。また、第二ハッシュテーブル $HASHTBL2$ に含まれる n 個の第二ハッシュ値とコンテンツ位置情報 POS に含まれる n 個のユニット数と配布データ領域特定情報 $AREA$ の値を連結した値に対する認証情報であっても良い。

【0106】

(17) 実施の形態 1 の可搬媒体 11 では、コンテンツ CNT は暗号化されて記録されていたが、可搬媒体 11 にはコンテンツ CNT をそのまま記録するようにしても良い。こ

うすることにより、実行装置１２で暗号化コンテンツＥＮＣＣＮＴを復号化する必要がなくなるといった効果が生まれる。

（１８）実施の形態１の実行装置１２のコンテンツ鍵取得部１２１２では、暗号化鍵束ＫＢ、及びデバイス鍵格納部１２１１に格納されている情報を用いて、コンテンツ鍵ＣＫを取得していたが、配布センタ１０がデバイス鍵格納部１２１１の代わりに、コンテンツ鍵ＣＫを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵取得部１２１２はコンテンツ鍵格納部からコンテンツ鍵を取得するようにしても良い。この場合、発行センタ１０は可搬媒体１１に暗号化鍵束ＫＢを記録する必要はなく、実行装置１２は暗号化鍵束ＫＢを受信する必要もない。こうすることにより、可搬媒体１１に暗号化鍵束ＫＢを記録しなくてすむため、記録データのサイズを削減することが出来る。

【０１０７】

（１９）実施の形態１の配布センタ１０は、可搬媒体１１を介して実行装置１２へコンテンツＣＮＴを配布していたが、これに限るものではない。例えば、配布センタ１０と実行装置１２がインターネット等の通信ネットワークに接続されており、配布センタ１０は、その通信ネットワークを介して実行装置１２へコンテンツＣＮＴを配布するようにしてもよい。もしくは、放送網を介して配布してもよい。

【０１０８】

（２０）実施の形態１の配布センタ１０の認証情報生成情報格納部１００９、及び、実行装置１２の検証情報格納部１２１５は、これに限るものではない。例えば、以下のような例が考えられる。

（ｉ）認証情報生成情報格納部１００９は、図２９で示すように、１つの認証情報生成情報ＧＥＮＡＵＴＨ_i（ＧＥＮＡＵＴＨ_１、・・・、ＧＥＮＡＵＴＨ_wのいずれか（wは１以上の自然数））と対応する検証情報識別子ＶＥＲＩＤ_iを保持しており、検証情報格納部１２１５は、図３０で示すように、w組の検証情報識別子（ＧＥＮＡＵＴＨ_１、・・・、ＧＥＮＡＵＴＨ_w）と、その検証情報識別子に対応する認証情報生成情報と対となる検証情報（ＶＥＲ_１、・・・、ＶＥＲ_w）を保持する。配布センタ１０の記録部１０１１は、可搬媒体１１に、認証情報生成情報格納部１００９に格納されている検証情報識別子ＧＥＮＡＵＴＨ_iを記録するようにして、実行装置１２の認証情報検証部１２１６は、可搬媒体１１に記録されている検証情報識別子ＧＥＮＡＵＴＨ_iに対応する検証情報ＶＥＲ_i（ＶＥＲ_１、・・・、ＶＥＲ_wのいずれか）を検証情報格納部１２１５から取得し、その検証情報ＶＥＲ_iを基に、認証情報ＡＵＴＨを検証するようにしてもよい。

【０１０９】

（ｉｉ）認証情報生成情報格納部１００９には、認証情報生成情報ＧＥＮＡＵＴＨと対応する検証情報ＶＥＲを保持しており、検証情報格納部１２１５は何も保持していない。配布センタ１０の記録部１０１１は、可搬媒体１１に、認証情報生成情報格納部１００９に格納されている検証情報ＶＥＲを加えて記録するようにして、実行装置１２の認証情報検証部１２１６は、可搬媒体１１に記録されている検証情報ＶＥＲを基に、認証情報ＡＵＴＨを検証する。

【０１１０】

（ｉｉｉ）認証情報生成情報格納部１００９には、図３１で示すように、認証情報生成情報ＧＥＮＡＵＴＨと対応する検証情報ＶＥＲ、及び、第三者機関によって生成された検証情報ＶＥＲに対する認証情報（例えばデジタル署名）であるセンタ認証情報ＣＡＵＴＨを保持しており、検証情報格納部１２１５は、図３２で示すように、第三者機関の検証情報であるセンタ検証情報ＣＶＥＲ（例えばデジタル署名の署名検証鍵）を保持している場合が考えられる。なお、第三者機関の具体例としては、信頼出来る第三者機関（Ｔｒｕｓｔｅｄ　Ｔｈｉｒｄ　Ｐａｒｔｙ）や、鍵配布センタなどである。この場合、配布センタ１０の記録部１０１１は、可搬媒体１１に、認証情報生成情報格納部１００９に格納されている検証情報ＶＥＲ及びセンタ認証情報ＣＡＵＴＨを記録するようにして、実行装置１２の認証情報検証部１２１６は、検証情報格納部１２１５のセンタ検証情報ＣＶＥＲを用いて、可搬媒体１１に記録されているセンタ認証情報ＣＡＵＴＨが、検証情報ＶＥＲに対

する第三者機関の正規の認証情報であるかどうか検証し、その検証が成功した場合に、その検証情報VERを基に、認証情報AUTHを検証する。

【0111】

これにより、配布センタ10が複数存在している場合にそれぞれの配布センタ10に別の検証情報を設定したとしても、実行装置12に予め各検証情報を保持しておく必要がなくなる。さらに、偽の認証情報が出回った場合にも、どの配布センタ10から漏洩したのか追跡することが出来る。

(21)変形例(20)において、実行装置12は、さらに、無効検証情報を外部から受信するようにしてもよい。例えば、変形例(20)の(i)の場合、無効検証情報には、検証情報識別子が含まれており、実行装置12には、外部から無効検証情報として検証情報識別子GENAUTHjを受信した場合に、検証情報格納部1215に格納されている検証情報識別子GENAUTHjに対応する検証情報VERjを無効化する検証情報無効化部を備えていてもよい。

【0112】

また、変形例(20)の(ii)及び(iii)の場合、無効検証情報には、検証情報が含まれており、実行装置12の検証情報格納部1215は、外部から受信した無効検証情報として検証情報を保持しており、認証情報検証部1216は、検証情報格納部1215の無効検証情報に、可搬媒体11に記録されている検証情報が含まれていないか確認を行い、含まれている場合は、コンテンツCNTの再生、実行開始を行わないようにしてもよい。

【0113】

なお、実行装置12が外部から無効検証情報を受信する方法としては、可搬媒体11や記録媒体に記録されている無効検証情報を受信する方法や、通信ネットワークや放送網から無効検証情報をダウンロードする方法などがある。これにより、万が一、ある配布センタの認証情報生成情報が不正者に漏洩したとしても、その認証情報生成情報に対応する検証情報を無効検証情報に含めることによって、その漏洩した認証情報生成情報を無効化することが実現出来る。

【0114】

(22)変形例(21)において、実行装置12は、最新の無効検証情報のみを検証情報格納部1215に保持するようにしてもよい。例えば、無効検証情報には発行日が記載されており、実行装置12は、検証情報格納部1215が保持する無効検証情報よりも発行日が新しい無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部1215に上書きするようにしてもよいし、また、無効検証情報には発行IDが記載されており、実行装置12は、検証情報格納部1215が保持する無効検証情報よりも発行IDが最新の無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部1215に上書きするようにしてもよい。

【0115】

(23)実施の形態1の実行装置12は、可搬媒体11内のコンテンツCNTを再生、実行開始する前に、そのコンテンツCNTが不正なものであるか検証していたが、それに限るものではない。例えば、可搬媒体11が光ディスクであり、実行装置12がディスクトレイを有している場合、可搬媒体11が実行装置12のディスクトレイに挿入された場合に、そのコンテンツCNTが不正なものであるか検証するようにしても良い。そうすることにより、ディスクトレイに挿入された可搬媒体11内のコンテンツCNTをイジェクトせずに何度も実行、再生する場合にでも、光ディスクの挿入時1度しか検証しないですむようになるため、コンテンツCNTの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体11がSDカード等の外部メモリで、実行装置12が外部メモリスロットを有している場合にも、同様のことが実現出来る。

【0116】

(24)実施の形態1の実行装置12の認証情報検証部1216においては、入替第二ハッシュテーブルを生成し、それを基に認証情報AUTHの正当性を検証していたが、こ

れに限るものではない。例えば、実行装置 1 2 の認証情報検証部 1 2 1 6 では、まず第一ステップとして、図 3 3 で示すように、可搬媒体 1 1 に記録されていた認証情報 A U T H が、同じく可搬媒体 1 1 に記録されていた第二ハッシュテーブル及びコンテンツ位置情報及び配布データ領域特定情報を結合した値に対する正規の認証情報であるか検証する。次に第二ステップとして、図 3 4 で示すように、選択された特定情報に対応する暗号化部分コンテンツの属性値が、特定情報に対応する第二ハッシュ値と等しいかどうか検証し、さらに、選択された第一識別子に対応するユニットの属性値が、第一識別子に対応する第一ハッシュ値と等しいかどうか検証するようにしてもよい。これにより、同様にコンテンツの正当性を検証することが出来る。暗号化部分コンテンツの属性値と第二ハッシュ値との検証については、図 3 5 に詳細を示している。また、ユニットの属性値と第一ハッシュ値との検証については、図 3 6 に詳細を示している。

【0 1 1 7】

(25) 実施の形態 1 において、可搬媒体 1 1 には第一ハッシュテーブル群と第二ハッシュテーブルとコンテンツ位置情報と配布データ領域特定情報と暗号化コンテンツとをそれぞれ一つずつ記録していたが、これに限るものではない。例えば、可搬媒体 1 1 には第一ハッシュテーブル群と第二ハッシュテーブルとコンテンツ位置情報と配布データ領域特定情報と暗号化コンテンツとを z 組 (z は 2 以上の自然数) 格納しても良い。このような場合、以下のようなことが実現出来る。例えば、可搬媒体 1 1 が光ディスクであり、実行装置 1 2 はディスクトレイを有しているとする。この場合、可搬媒体 1 1 が実行装置 1 2 のディスクトレイに挿入された時に、 z 組全てのコンテンツ位置情報からいくつかの特定情報を選択し検証を行うようにする。そして、 z 個ある暗号化コンテンツの中の一つのコンテンツを実行、再生開始する前に、そのコンテンツに対応するコンテンツ位置情報の中からいくつかの特定情報を選択し検証を行うようにする。こうして、可搬媒体 1 1 が実行装置 1 2 のディスクトレイに挿入された場合に一度のみ、多くの数の特定情報の検証を行い、各コンテンツを実行、再生開始する際には、ディスクトレイに挿入された時よりも少ない数の特定情報に対して検証するようにする。これにより、ディスクトレイに挿入された可搬媒体 1 1 内のコンテンツを何度も実行する場合に、コンテンツの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体 1 1 は光ディスクでなくてもよく、例えば S D カード等の外部メモリであっても同様のことが実現出来る。

【0 1 1 8】

(26) 実施の形態 1 においては、実行装置 1 2 の認証情報検証部 1 2 1 6 では、検証が成功した場合にのみ、実行部 1 2 1 7 へ実行許可情報 P E R M を出力していたが、これに限るものではない。例えば、実行部 1 2 1 7 は、コンテンツ鍵取得部 1 2 1 2 からコンテンツ鍵を入力された場合に、可搬媒体 1 1 に記録された暗号化コンテンツを逐次取得、復号化、実行もしくは再生するようにして、認証情報検証部 1 2 1 6 は、検証が失敗した場合に、実行部 1 2 1 7 へ実行不許可情報 N O T P E R M を出力するようにして、実行部 1 2 1 7 は認証情報検証部 1 2 1 6 から実行不許可情報 N O T P E R M を入力された場合、実行もしくは再生を停止するようにしてもよい。こうすることにより、コンテンツを実行、再生開始するまでの時間を短縮することが出来るようになる。

【0 1 1 9】

もしくは、実行装置 1 2 の認証情報検証部 1 2 1 6 は、検証が成功した場合に実行部 1 2 1 7 へ実行許可情報 P E R M を出力し、検証が失敗した場合に実行部 1 2 1 7 へ実行不許可情報 N O T P E R M を出力するようにしてもよい。さらに、実行不許可情報 N O T P E R M を入力された実行部 1 2 1 7 では、外部に不正なコンテンツである旨メッセージを出力(例えば、ディスプレイに「不正なコンテンツです」と表示する)するようにしてもよい。実行不許可情報 N O T P E R M を入力された実行部 1 2 1 7 では、暗号化コンテンツ E N C C N T の復号化及び実行、再生を停止するのではなく、暗号化コンテンツ E N C C N T の復号化及び実行、再生は通常通り行うが、同時に外部に警告を出力(例えば、ディスプレイに「警告：不正なコンテンツです」と表示する)するようにしてもよい。また、実行装置 1 2 とサーバ(配布センタ 1 0 や別のセンタ)とが通信ネットワーク等で接続

されていて、不正コンテンツである旨をそのサーバに通知するようにしてもよい。また、実行装置１２では以後、あらゆる暗号化コンテンツＥＮＣＲＹＰＴの復号化及び実行、再生を禁止するような状態になってもよい。また、実行装置１２は、不正コンテンツを識別するコンテンツ識別情報（例えば、コンテンツ識別子）を装置内に記録するようにして、一定期間内、もしくは、永久的に、コンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、実行装置１２は、同じコンテンツ識別情報（例えば、コンテンツ識別子）を持つコンテンツがある一定回数以上認証に失敗した場合、一定期間内、もしくは、永久的に、そのコンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、可搬媒体１１が光ディスクであり、実行装置１２がディスクトレイを有している場合、可搬媒体１１がディスクトレイから排出されるようにしてもよい。

【０１２０】

（２７）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、リムーバブルディスク、ハードディスク、ＣＤ、ＭＯ、ＤＶＤ、ＳＤメモ리카ード、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とする通信ネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記通信ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【０１２１】

（２８）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【０１２２】

本発明にかかる不正コンテンツ検知システムは、実行装置においてコンテンツを実行開始、もしくは再生開始する前に、そのコンテンツが想定する主体（例えば正規の著作権を有する人／団体／会社や、正規のディスク製造業者、正規のディスクプレス業者など）により配布されたコンテンツかどうかを検知できるという機能を有し、その検知結果によりコンテンツの実行開始、再生開始を制御（例えば警告を表示する、コンテンツの実行／再生を停止する、コンテンツの実行／再生を禁止するなど）することが出来る。これは、コンテンツの著作権保護が必要とされるシステム全般、特に記録媒体や可搬媒体（例えば光ディスクやメモ리카ード）や通信ネットワーク、放送網を用いたコンテンツ配布システムに有用である。

【０１２３】

さらに、本発明は、動画データや音声データなどのマルチメディアコンテンツに限らず、コンテンツの実行順序を制御する実行順序ファイル（ナビゲーションファイル）や、コンピュータプログラム等の保護にも適用可能である。この場合、実行装置において、不正なコンピュータプログラム（例えばコンピュータウイルスを含むコンピュータプログラム）を実行開始しない等が実現出来る。そのため、安全（セキュア）な処理環境を実現するコンピュータシステム全般、特にＯＳ（Ｏｐｅｒａｔｉｏｎ Ｓｙｓｔｅｍ）等としても有用である。

【図面の簡単な説明】

【 0 1 2 4 】

【図 1】 本発明の実施の形態 1 における不正コンテンツ検知システムの概要図

【図 2】 本発明の実施の形態 1 における配布センタ 1 0 の構成例を示す図

【図 3】 本発明の実施の形態 1 における実行装置情報格納部 1 0 0 3 の構成例を示す図

【図 4】 本発明の実施の形態 1 における暗号化鍵束 K B の一例を示す図

【図 5】 本発明の実施の形態 1 における暗号化コンテンツ E N C C N T の作成方法の一例を示す図

【図 6】 本発明の実施の形態 1 における第一ハッシュテーブル群 H A S H T B L 1 G 及び、第二ハッシュテーブル H A S H T B L 2 の作成方法の一例を示す図

【図 7】 本発明の実施の形態 1 における第一ハッシュテーブル H A S H T B L 1 # 1 の作成方法の一例を示す図

【図 8】 本発明の実施の形態 1 における第二ハッシュテーブル H A S H T B L 2 の作成方法の一例を示す図

【図 9】 本発明の実施の形態 1 におけるコンテンツ位置情報 P O S の一例を示す図

【図 1 0】 本発明の実施の形態 1 における可搬媒体イメージ I M G の一例

【図 1 1】 本発明の実施の形態 1 における認証情報 A U T H の作成方法の一例を示す図

【図 1 2】 本発明の実施の形態 1 における第二可搬媒体イメージ I M G 2 の一例

【図 1 3】 本発明の実施の形態 1 における配布センタ 1 0 の処理の流れ図（一例）

【図 1 4】 本発明の実施の形態 1 における可搬媒体 1 1 に記録されるデータの一例

【図 1 5】 本発明の実施の形態 1 における実行装置 1 2 の構成例を示す図

【図 1 6】 本発明の実施の形態 1 におけるコンテンツ位置情報 P O S から i 組の特定情報とユニット数を選択する場合の一例を示す図

【図 1 7】 本発明の実施の形態 1 における入替第二ハッシュテーブル R E P H A S H T B L 2 の作成方法の一例を示す図

【図 1 8】 本発明の実施の形態 1 における入替第一ハッシュテーブル R E P H A S H T B L 1 # 1 の作成方法の一例を示す図

【図 1 9】 本発明の実施の形態 1 における入替第二ハッシュテーブル R E P H A S H T B L 2 の作成方法の一例を示す図

【図 2 0】 本発明の実施の形態 1 における認証情報 A U T H の検証方法の一例を示す図

【図 2 1】 実行装置 1 2 の処理の一例を示す流れ図

【図 2 2】 プログラムを処理するコンピュータの例

【図 2 3】 不正コンテンツ検知システムの別の一例

【図 2 4】 可搬媒体 1 1 に記録されるデータの別の一例を示す図

【図 2 5】 可搬媒体 1 1（光ディスク）と読取部 1 2 0 1 の一例を示す図

【図 2 6】 コンテンツ位置情報 P O S の別の一例を示す図

【図 2 7】 認証情報 A U T H の作成方法の別の一例を示す図

【図 2 8】 認証情報 A U T H の検証方法の別の一例を示す図

【図 2 9】 認証情報生成情報格納部 1 0 0 9 の別の一例を示す図

【図 3 0】 検証情報格納部 1 2 1 5 の別の一例を示す図

【図 3 1】 認証情報生成情報格納部 1 0 0 9 の別の一例を示す図

【図 3 2】 検証情報格納部 1 2 1 5 の別の一例を示す図

【図 3 3】 認証情報 A U T H の別の検証方法の一例（ステップ 1）を示す図

【図 3 4】 認証情報 A U T H の別の検証方法の一例（ステップ 2）を示す図

【図 3 5】 認証情報 A U T H の別の検証方法の一例（ステップ 2 の詳細 1）を示す図

【図 3 6】 認証情報 A U T H の別の検証方法の一例（ステップ 2 の詳細 2）を示す図

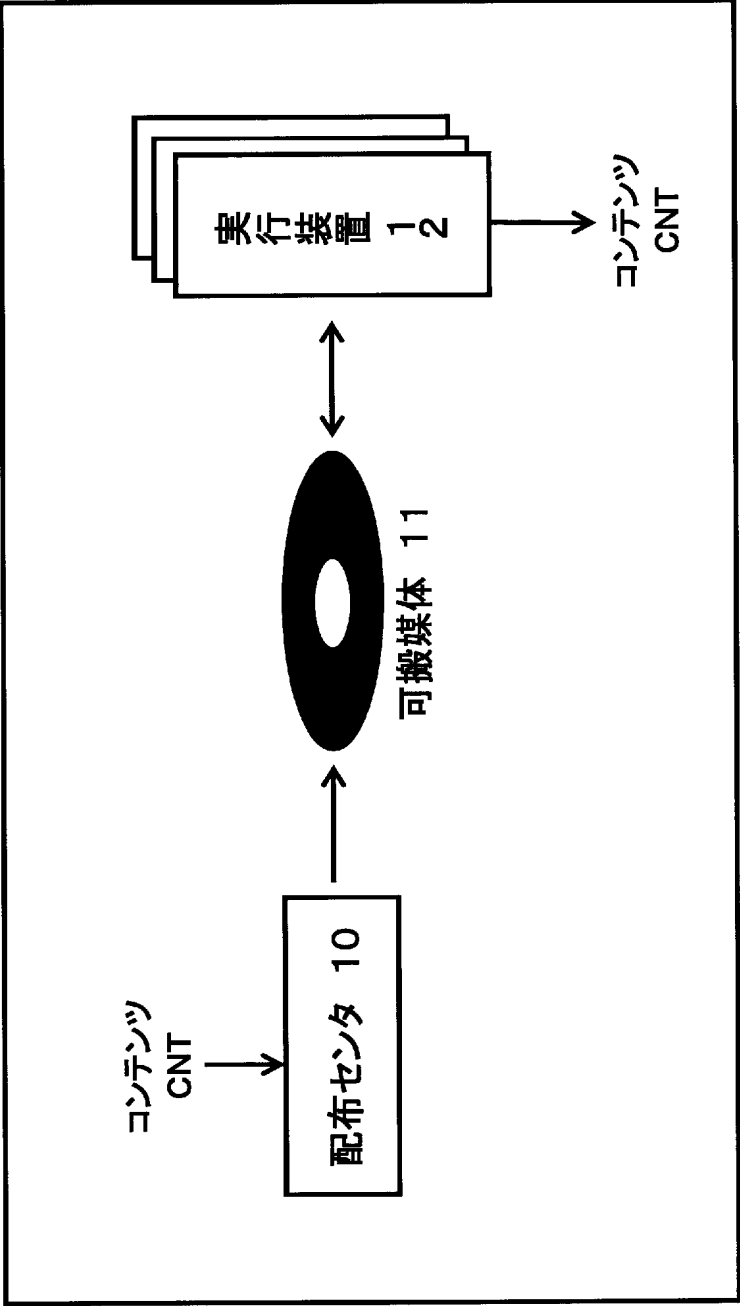
【図 3 7】 従来技術の可搬媒体に記録されるデータの構成を示す図

【符号の説明】

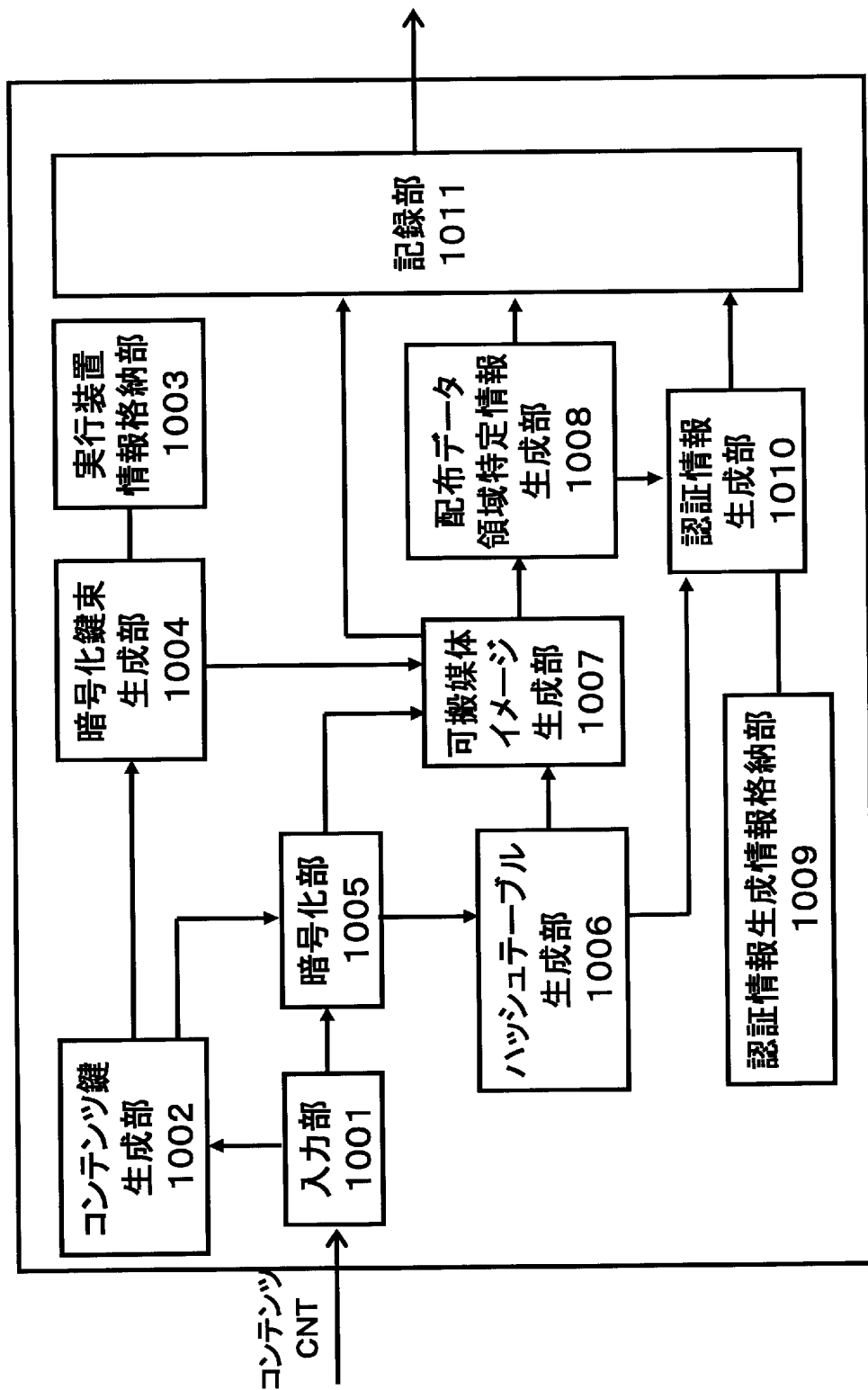
【 0 1 2 5 】

1 0	配布センタ
1 1	可搬媒体
1 2	実行装置
1 0 0 1	入力部
1 0 0 2	コンテンツ鍵生成部
1 0 0 3	実行装置情報格納部
1 0 0 4	暗号化鍵束生成部
1 0 0 5	暗号化部
1 0 0 6	ハッシュテーブル生成部
1 0 0 7	可搬媒体イメージ生成部
1 0 0 8	配布データ領域特定情報生成部
1 0 0 9	認証情報生成情報格納部
1 0 1 0	認証情報生成部
1 0 1 1	記録部
1 2 0	ドライブ部
1 2 1	コンテンツ実行部
1 2 0 1	取得部
1 2 0 2	配布データ領域特定情報格納部
1 2 0 3	第一秘密鍵格納部
1 2 0 4	第一秘匿通信処理部
1 2 1 1	デバイス鍵格納部
1 2 1 2	コンテンツ鍵取得部
1 2 1 3	第二秘密鍵格納部
1 2 1 4	第二秘匿通信処理部
1 2 1 5	検証情報格納部
1 2 1 6	認証情報検証部
1 2 1 7	実行部

不正コンテンツ検知システム1



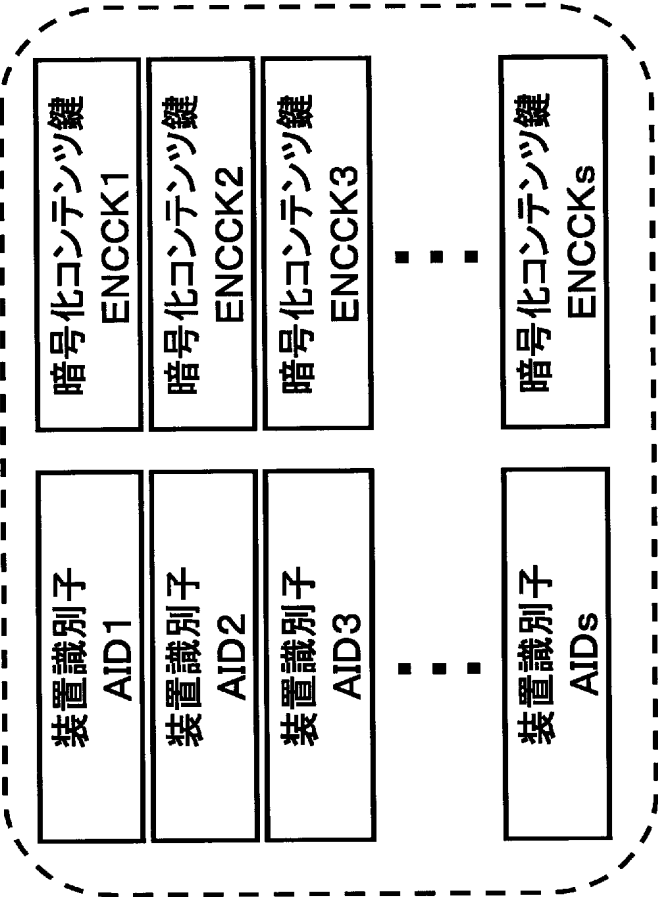
記録センタ 10 の一例



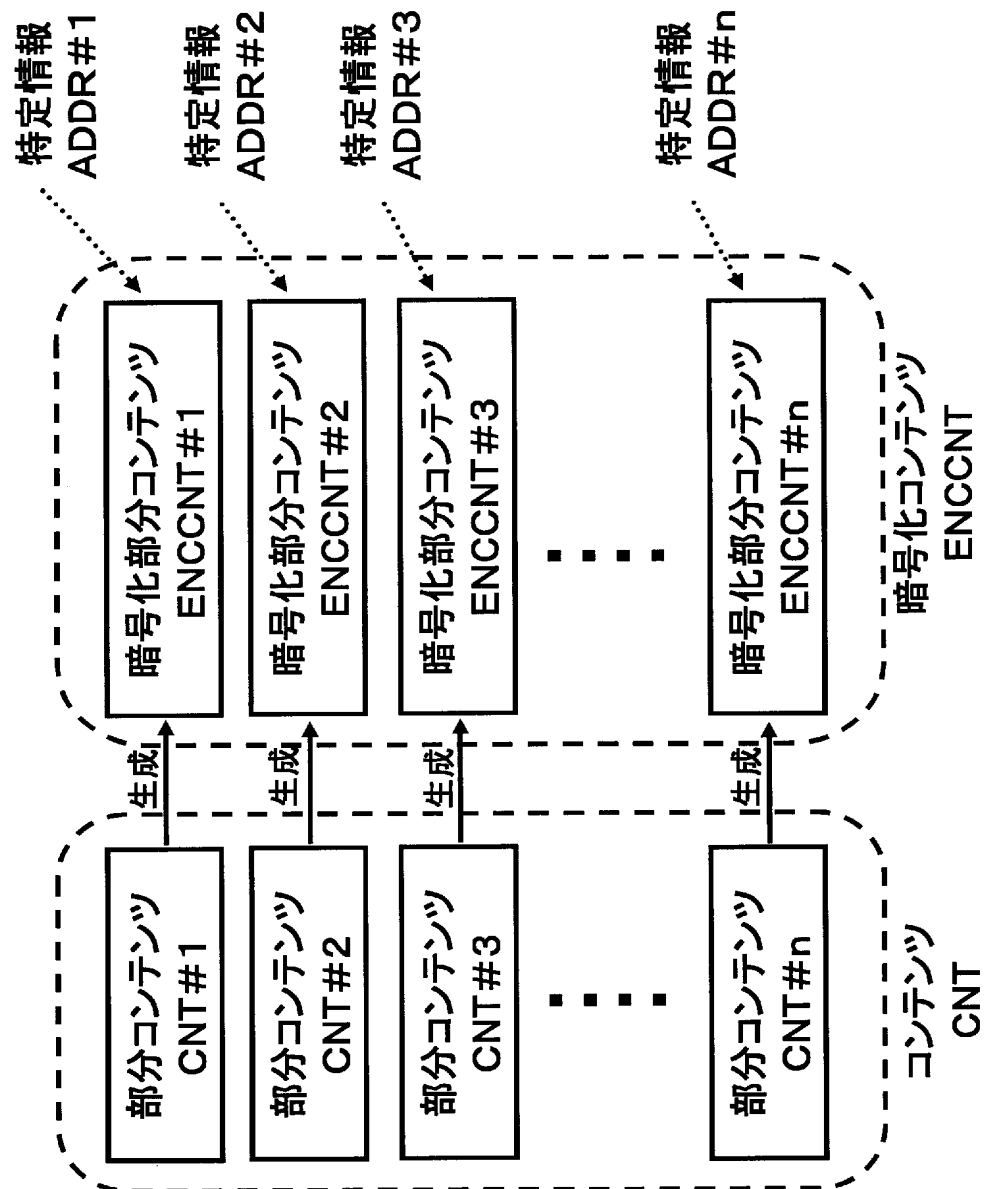
実行装置情報格納部1003の一例

装置識別子 AID1	デバイス鍵 DK1
装置識別子 AID2	デバイス鍵 DK2
装置識別子 AID3	デバイス鍵 DK3
■ ■ ■	■ ■ ■
装置識別子 AIDs	デバイス鍵 DKs

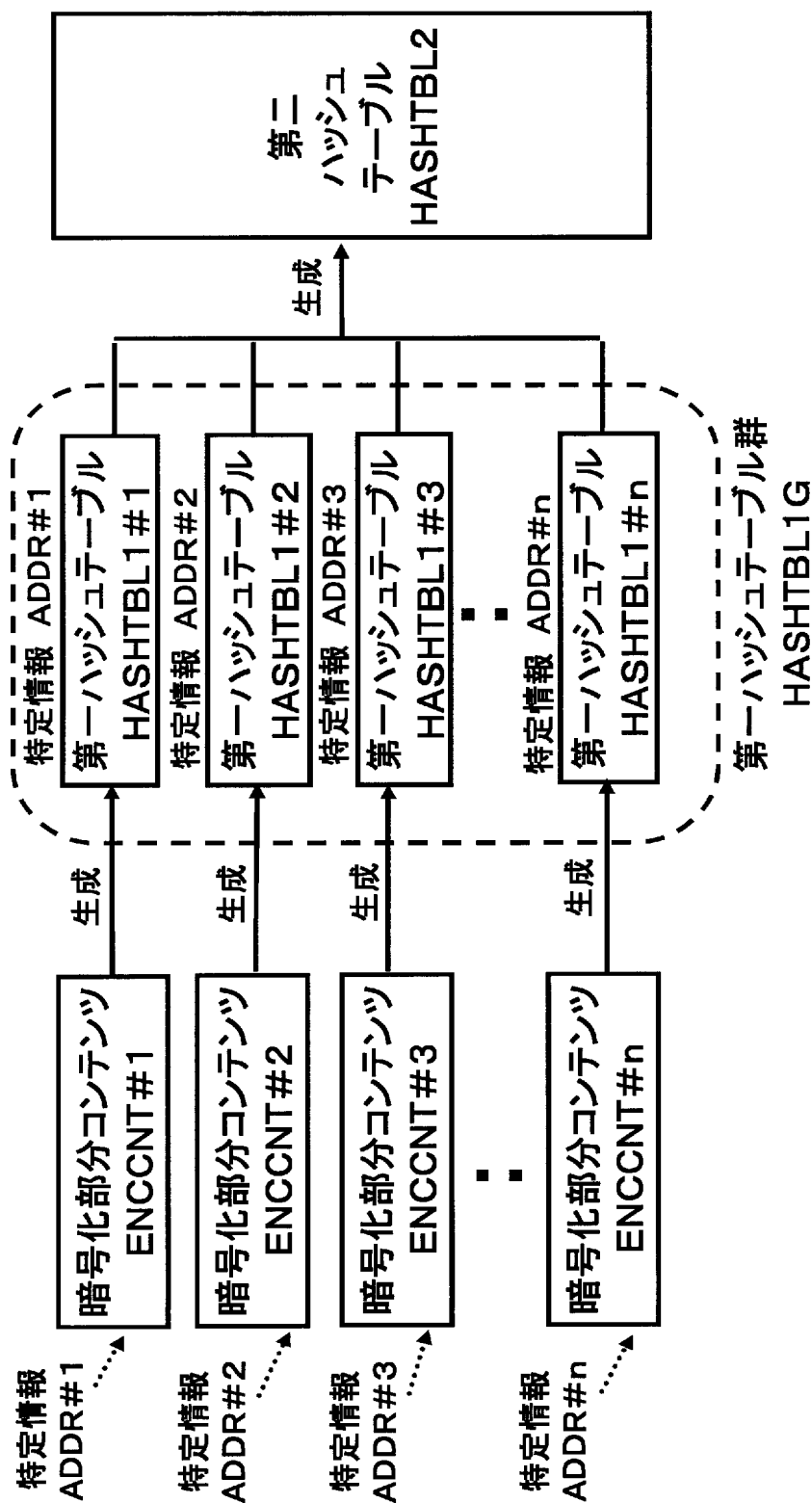
暗号化鍵束 KBの一例



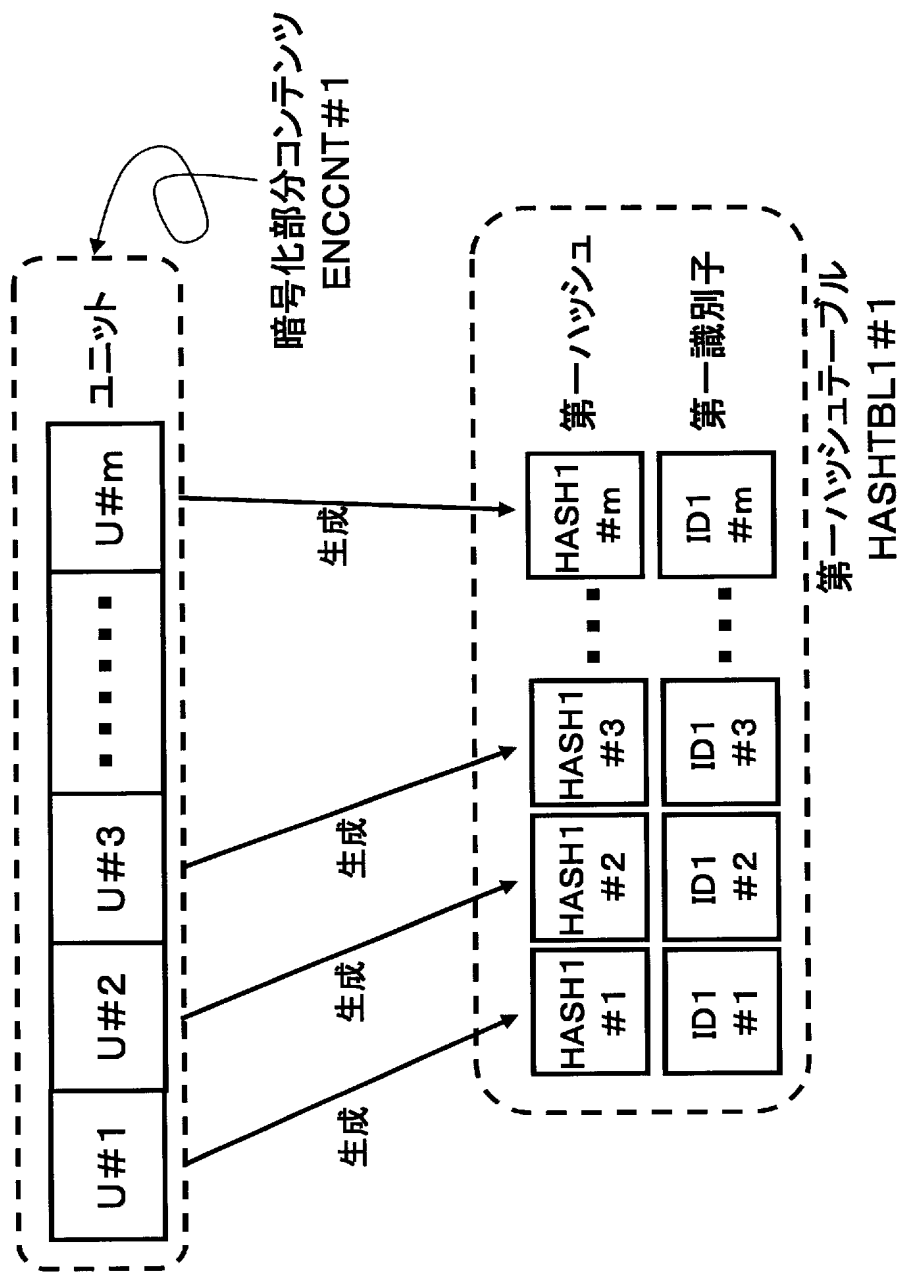
暗号化コンテンツENCNTの作成方法の一例



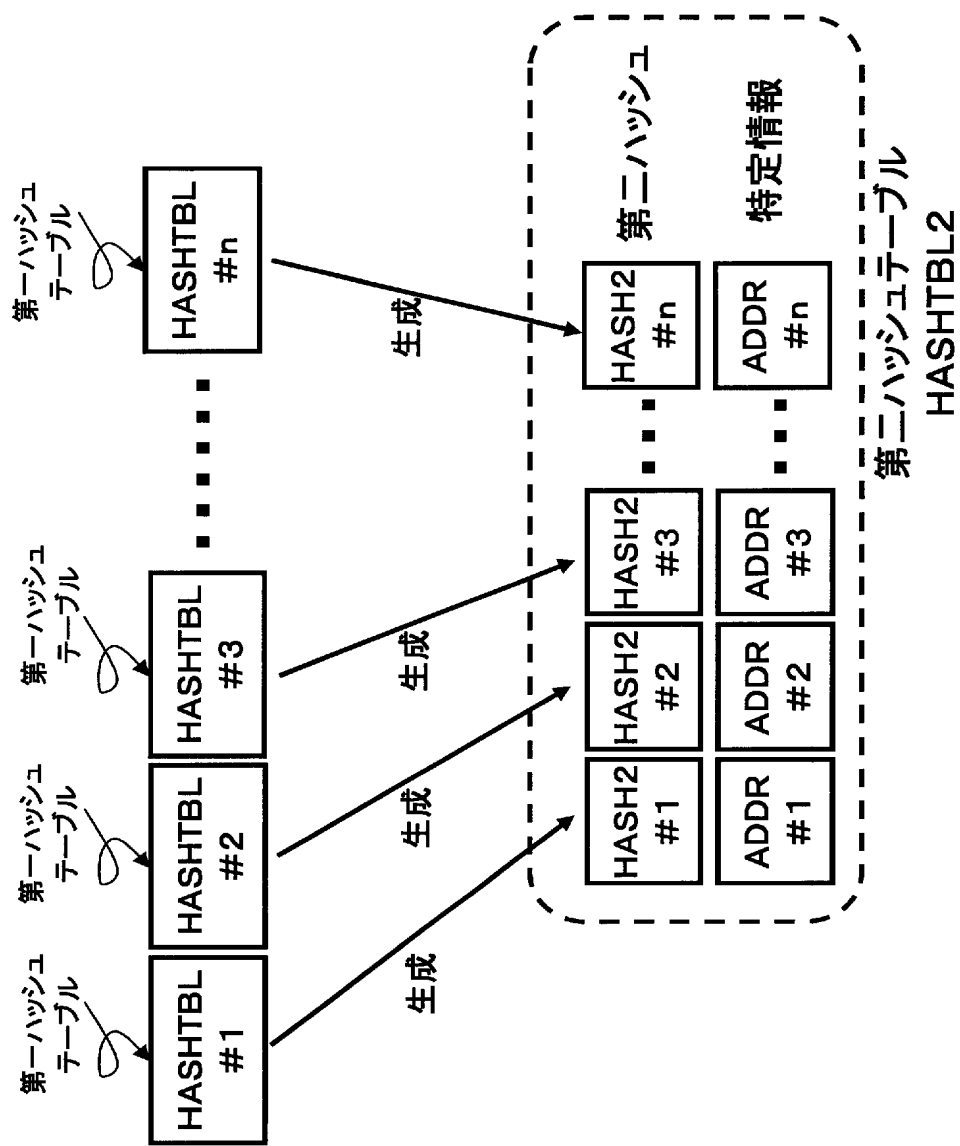
第一ハッシュテーブル群HASHTBL1G
及び、第二ハッシュテーブルHASHTBL2の作成方法の一例



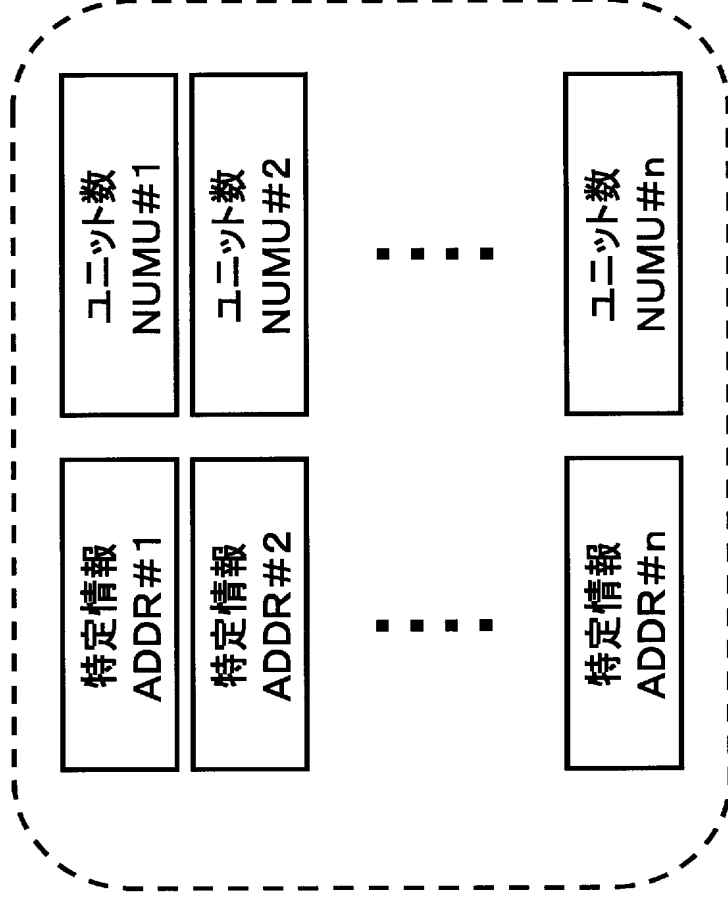
第一ハッシュテーブル HASHTBL1#1の作成方法の一例



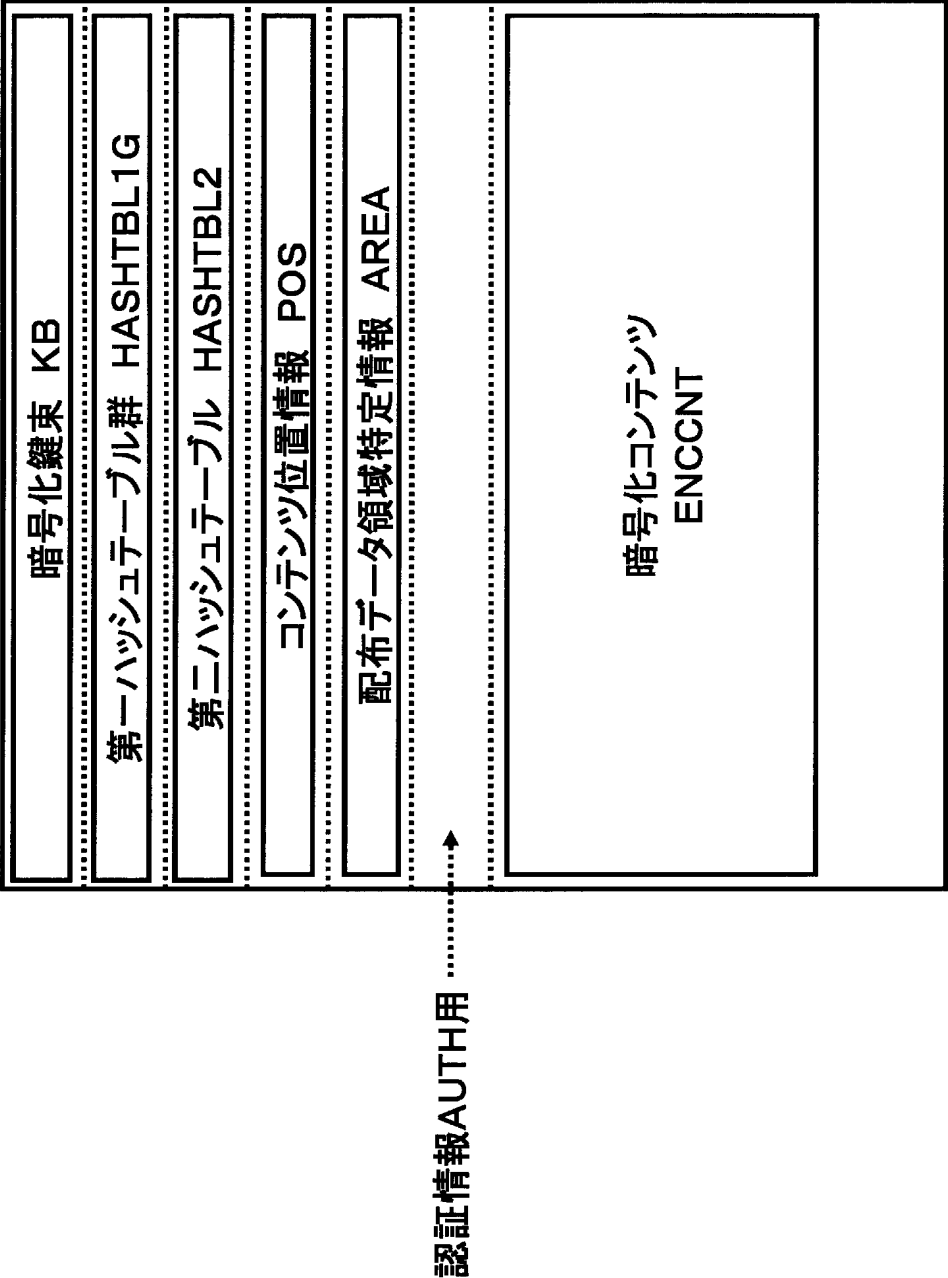
第二ハッシュテーブル HASHTBL2の作成方法の一例



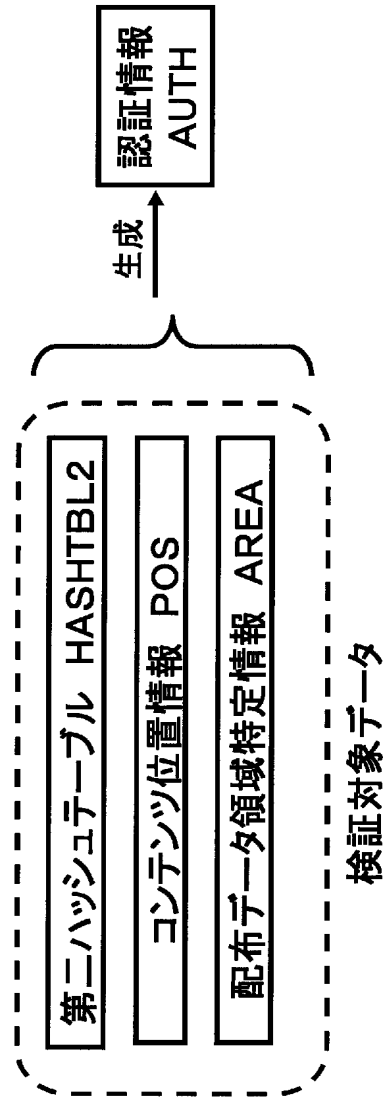
コンテンツ位置情報 POSの一例



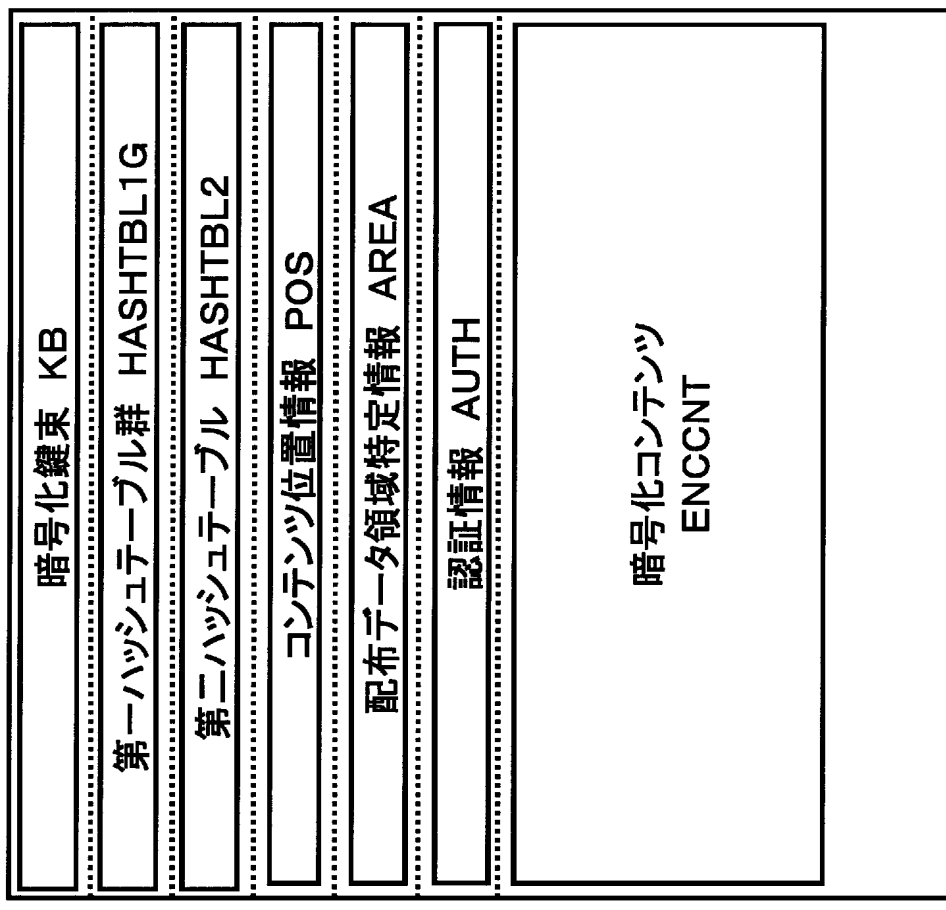
可搬媒体イメージIMGの一例

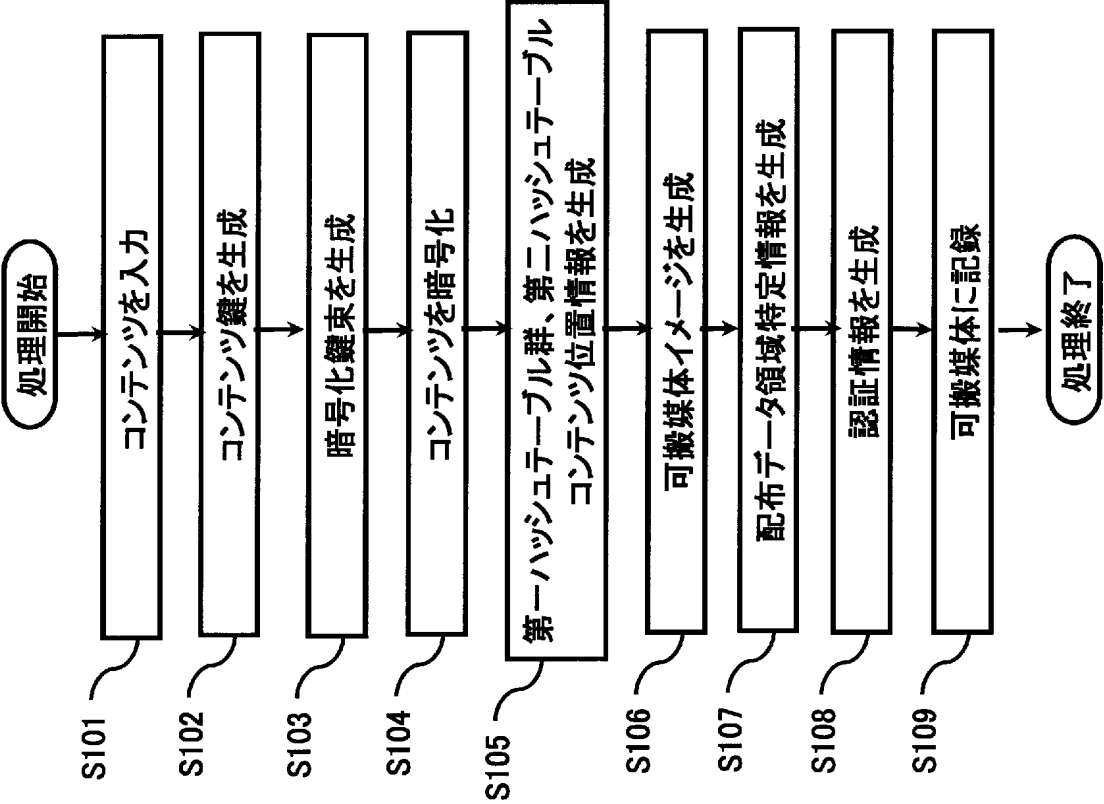


認証情報AUTHの作成方法の一例

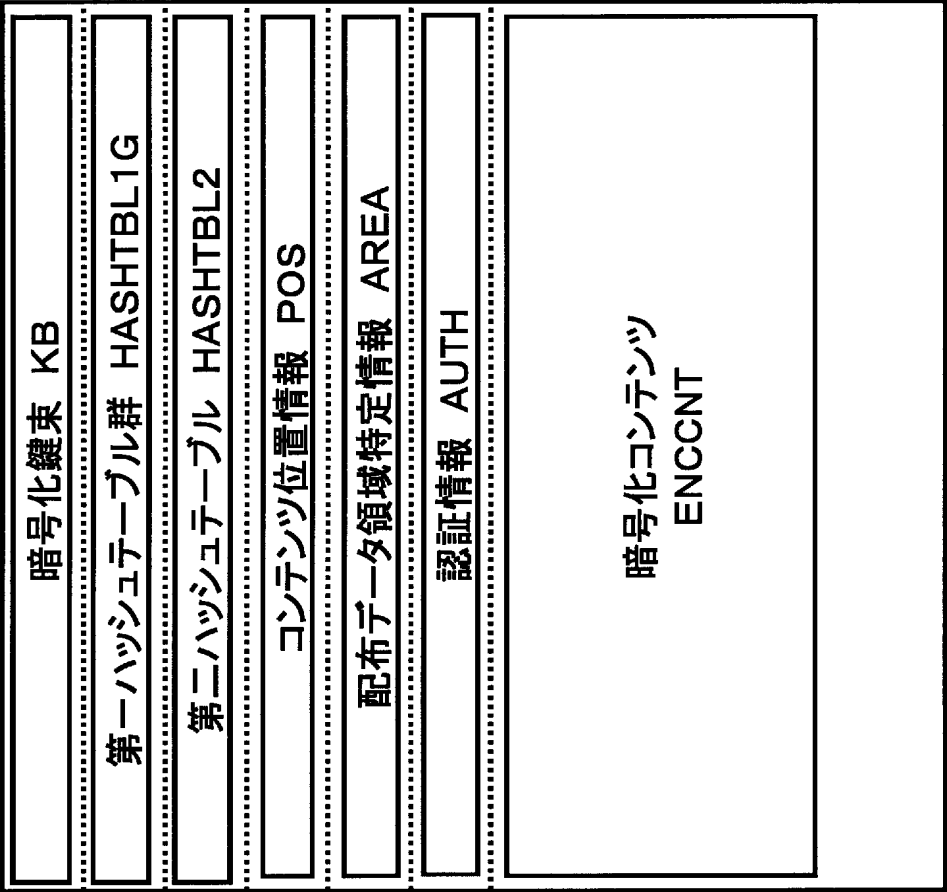


第二可搬媒体イメージIMG2の一例

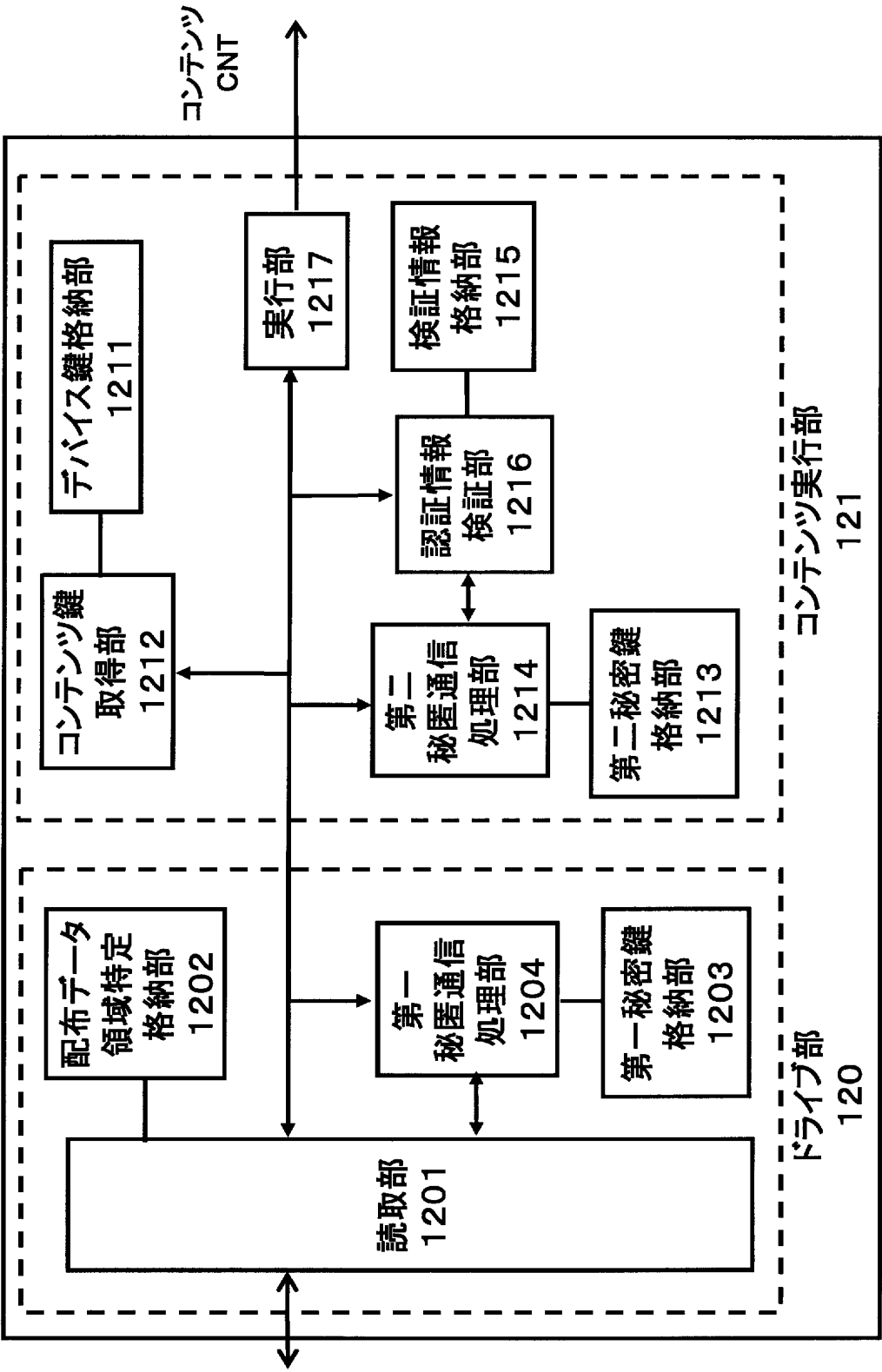


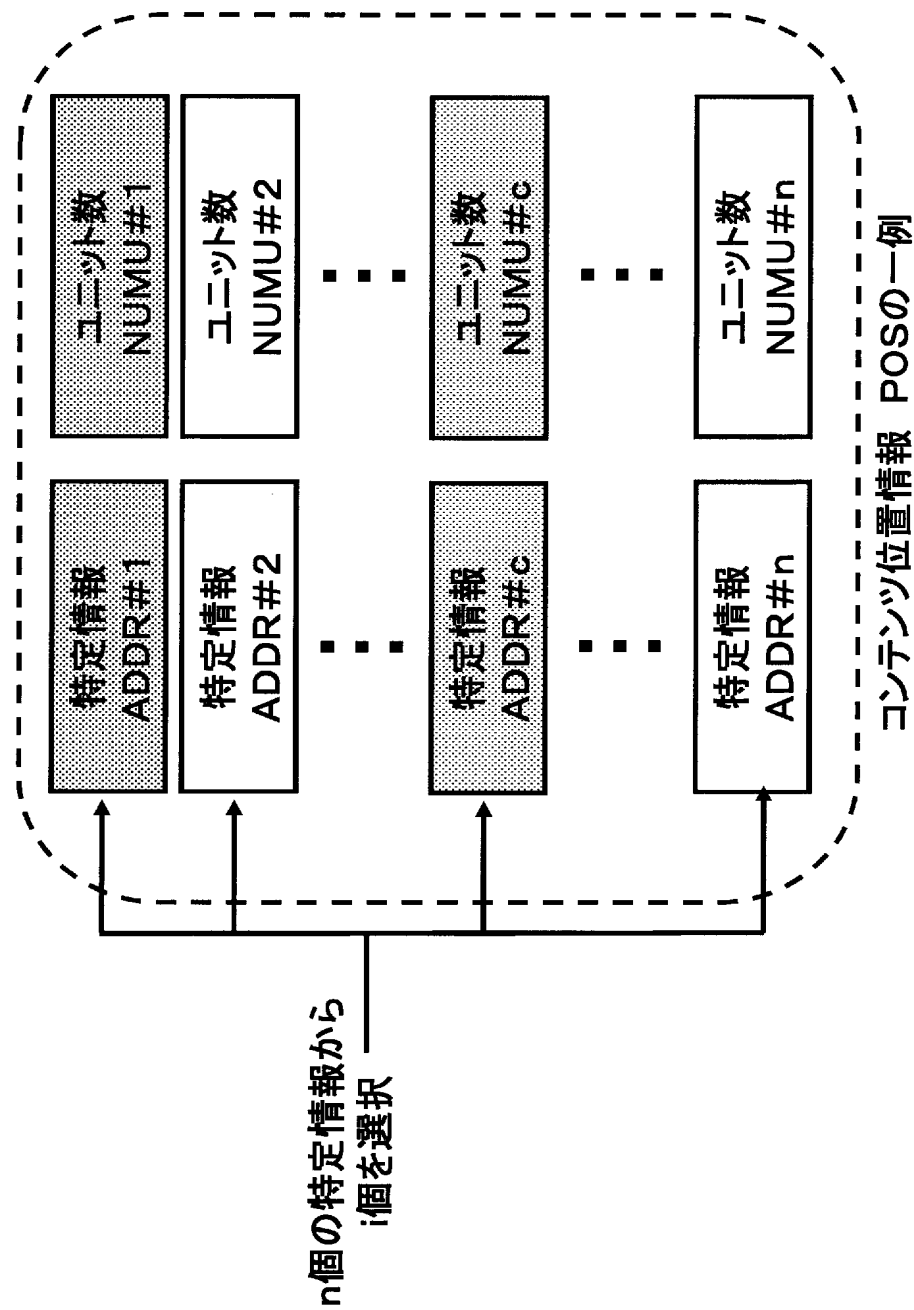


可搬媒体11に記録されるデータの一例

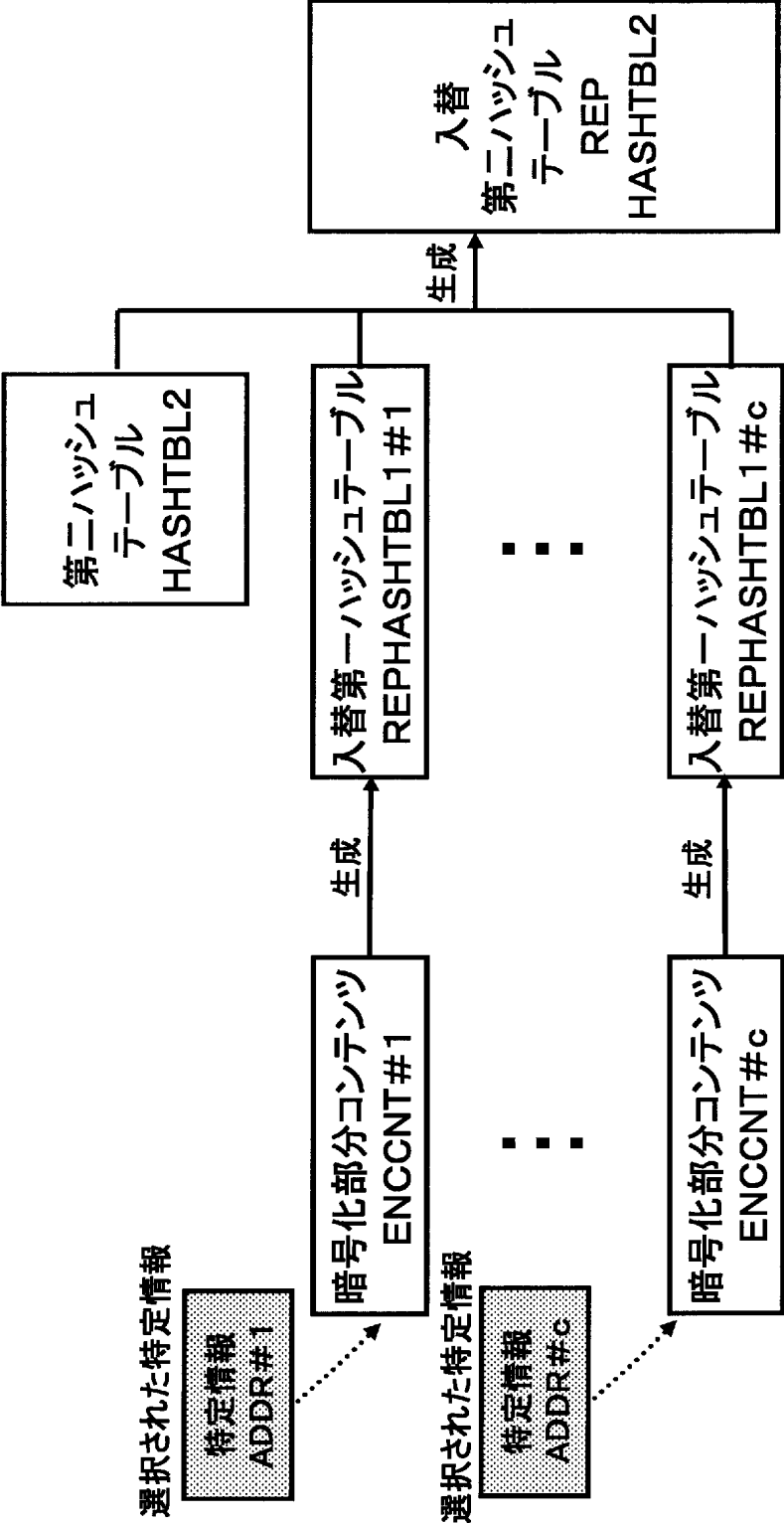


実行装置 12 の一例

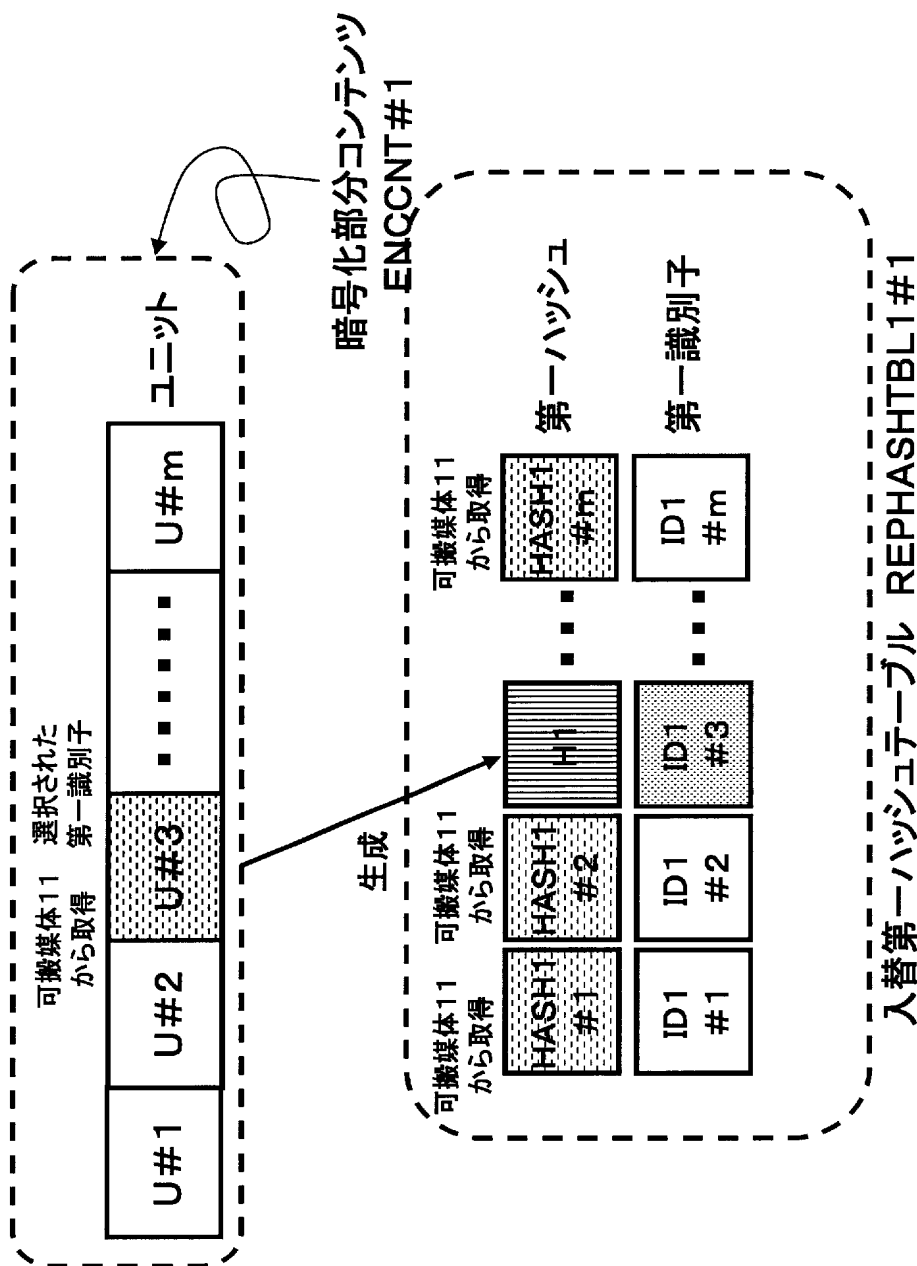




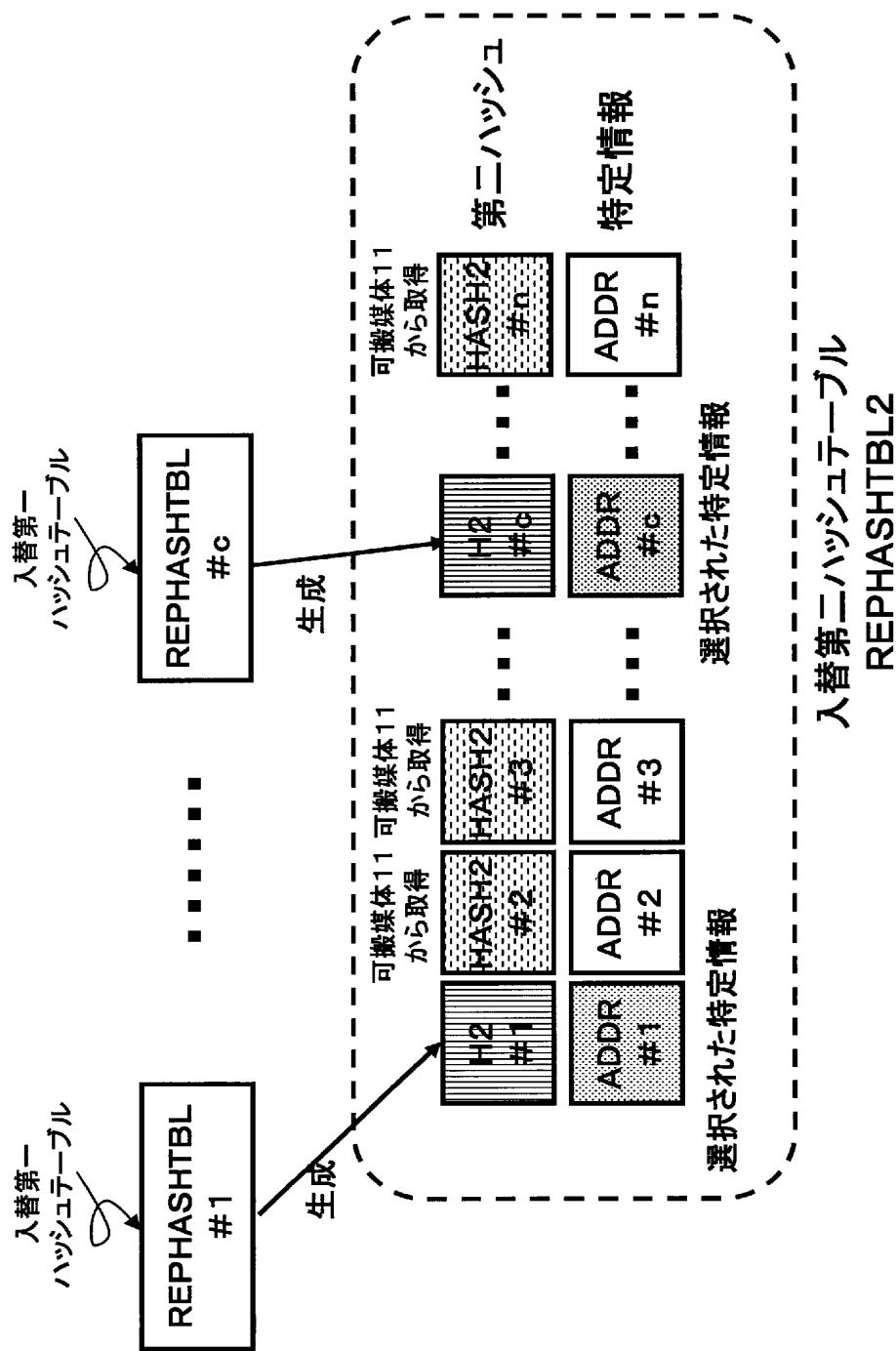
入替第二ハッシュテーブルREPHASHTBL2の作成方法の一例



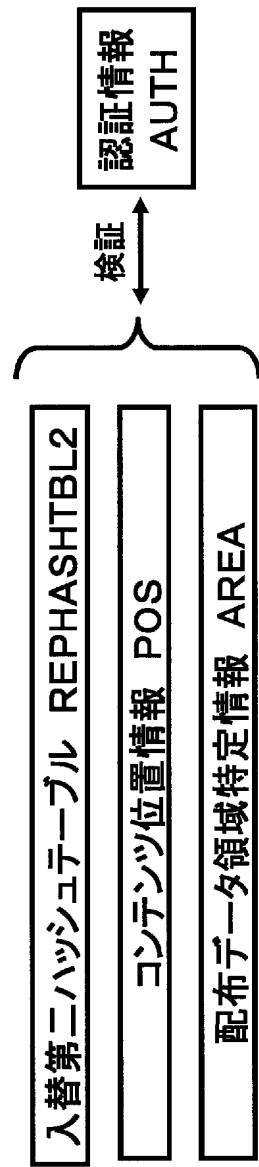
入替第一ハッシュテーブル REPHASHTBL1#1の作成方法の一例

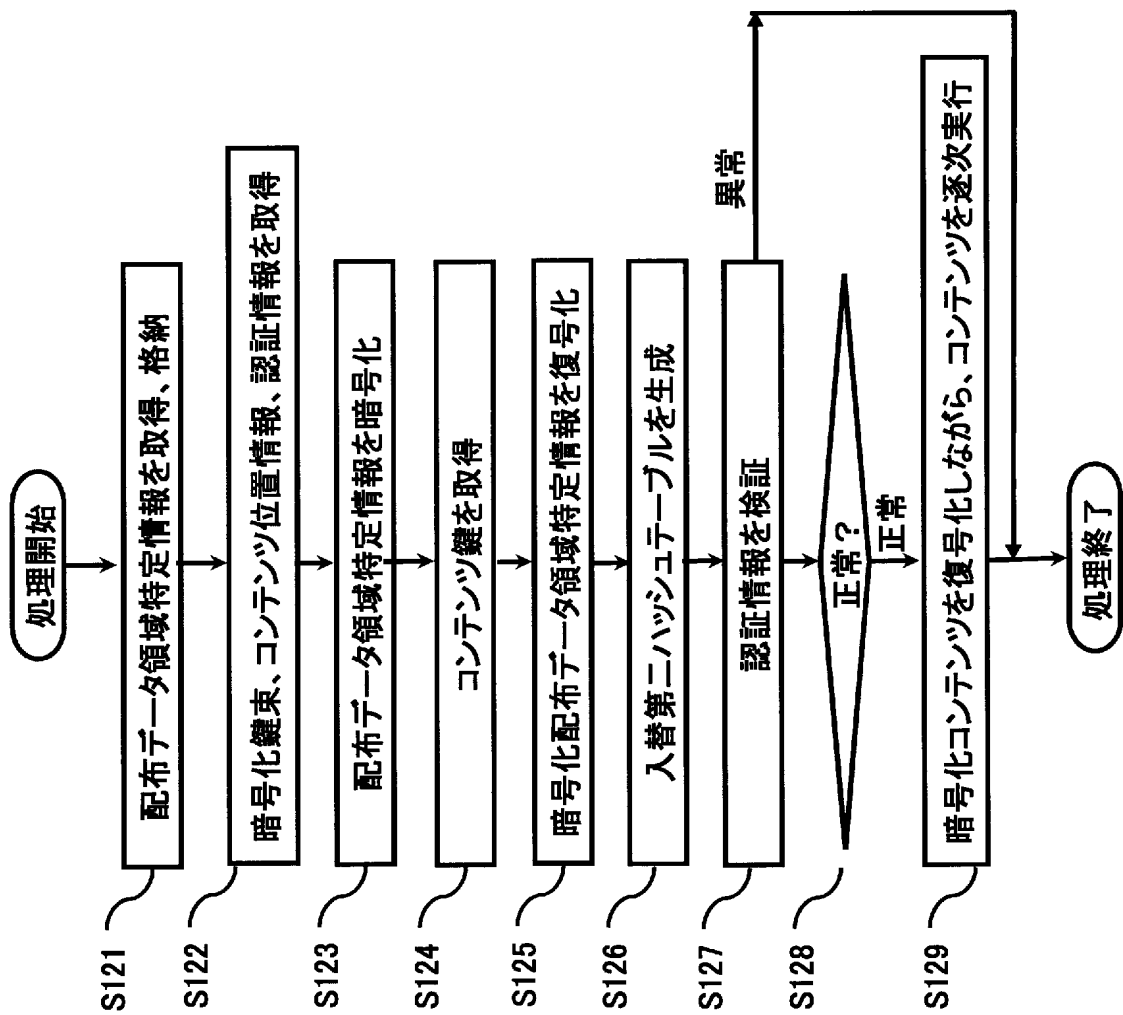


入替第二ハッシュテーブル REPHASHTBL2の作成方法の一例

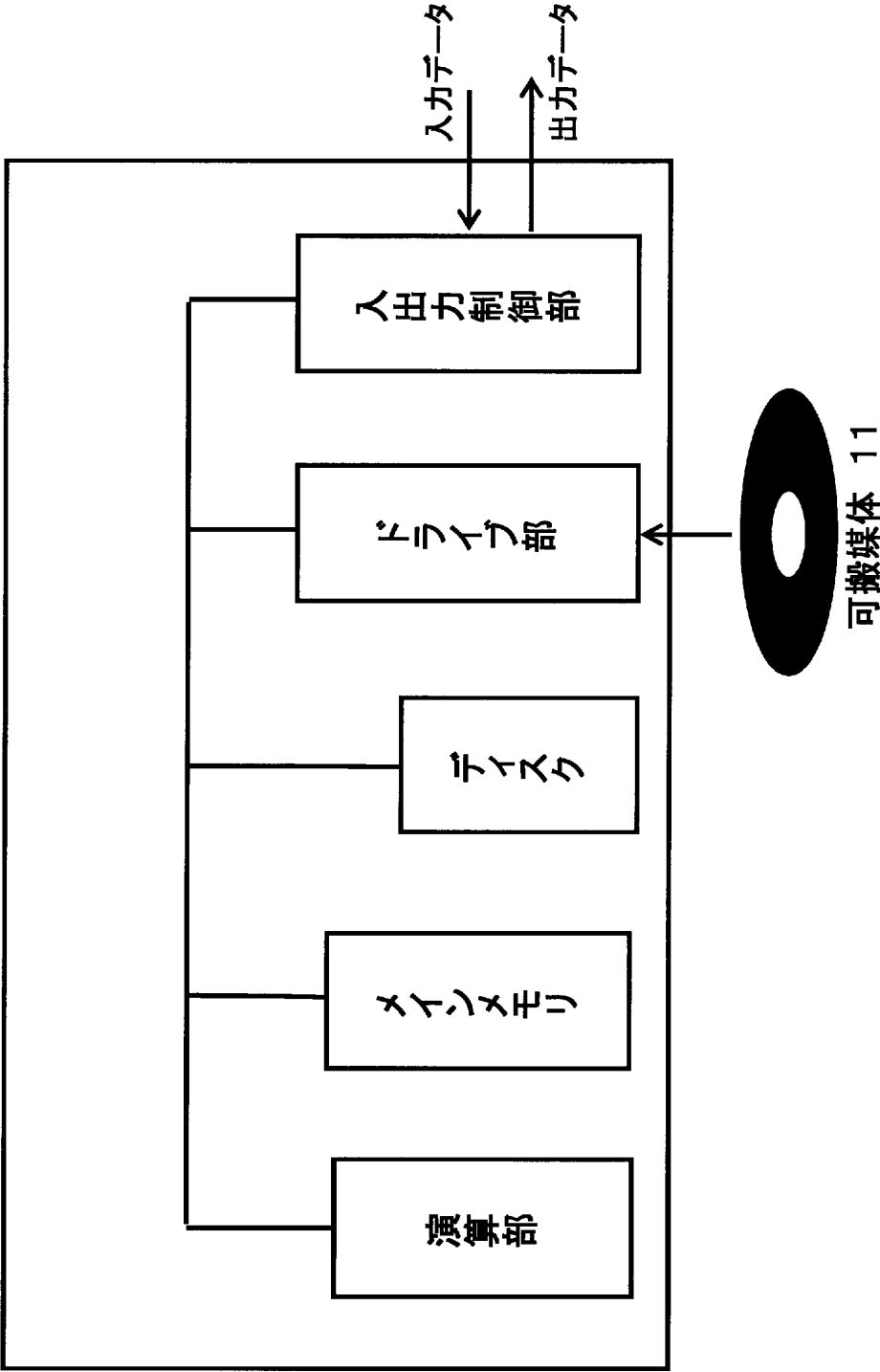


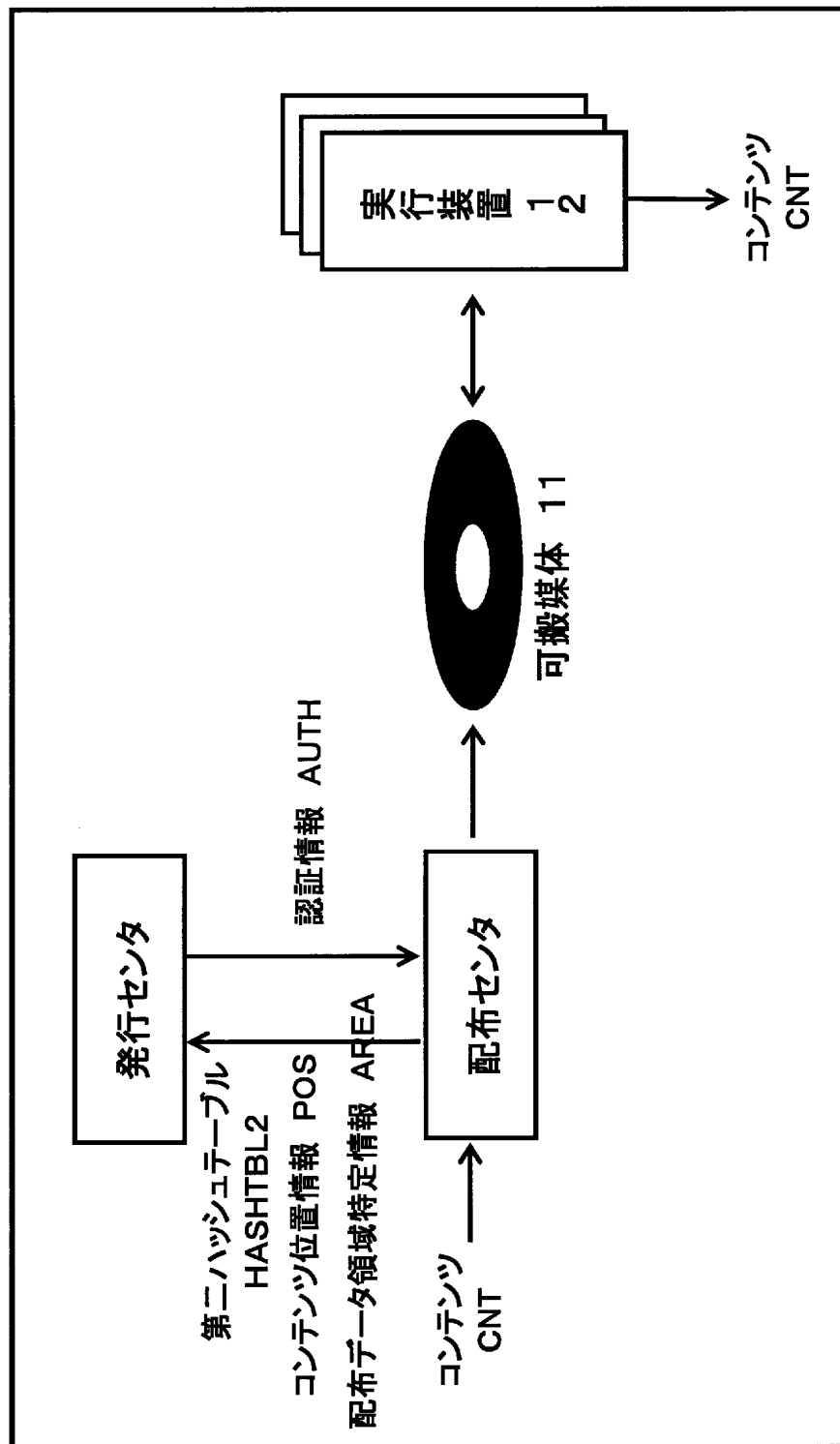
認証情報AUTHの検証方法の一例





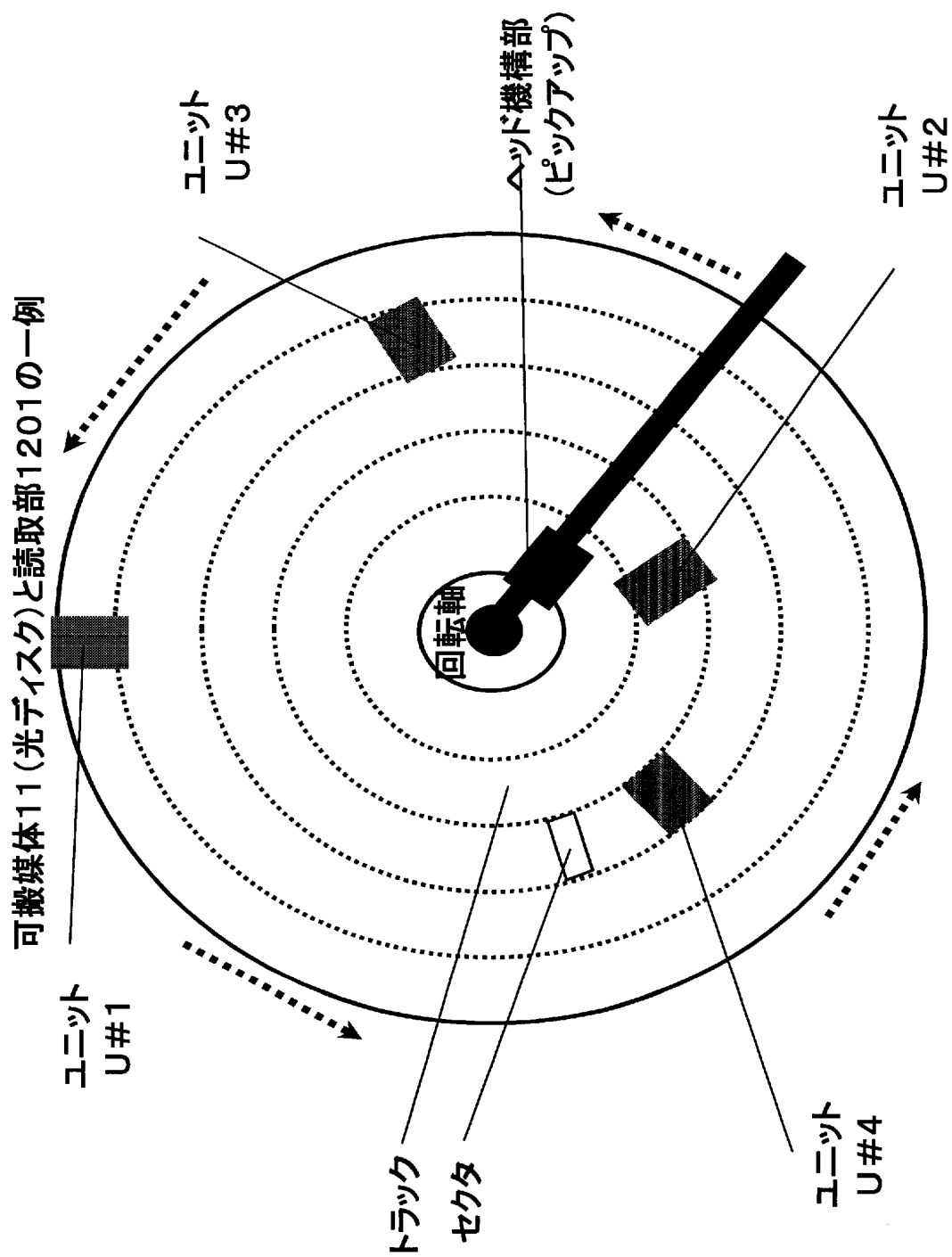
プログラムを処理するコンピュータの例



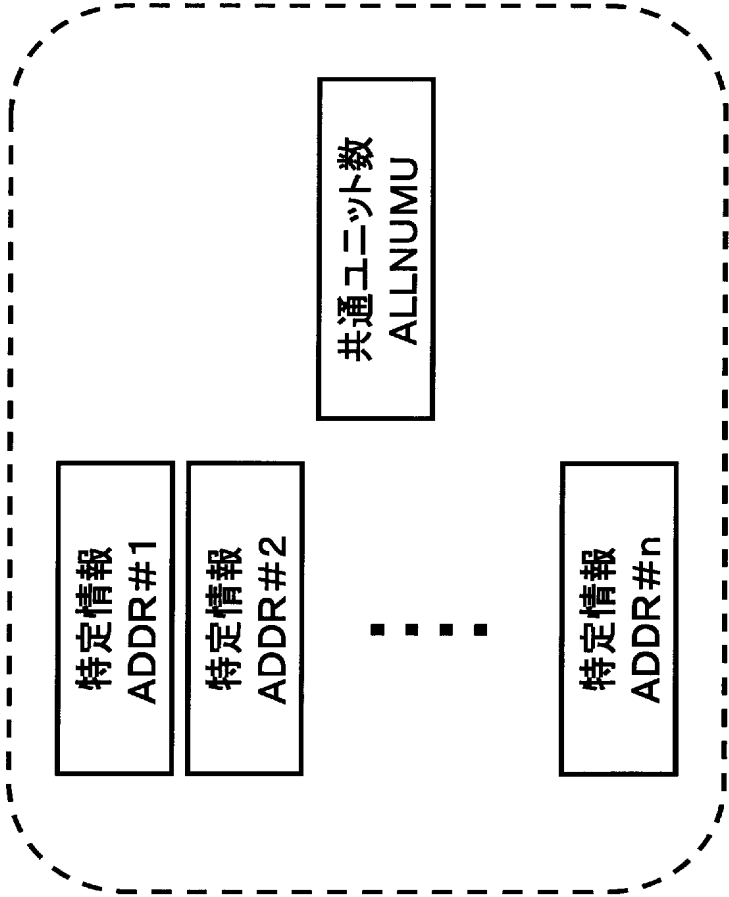


可搬媒体111に記録されるデータの別の一例

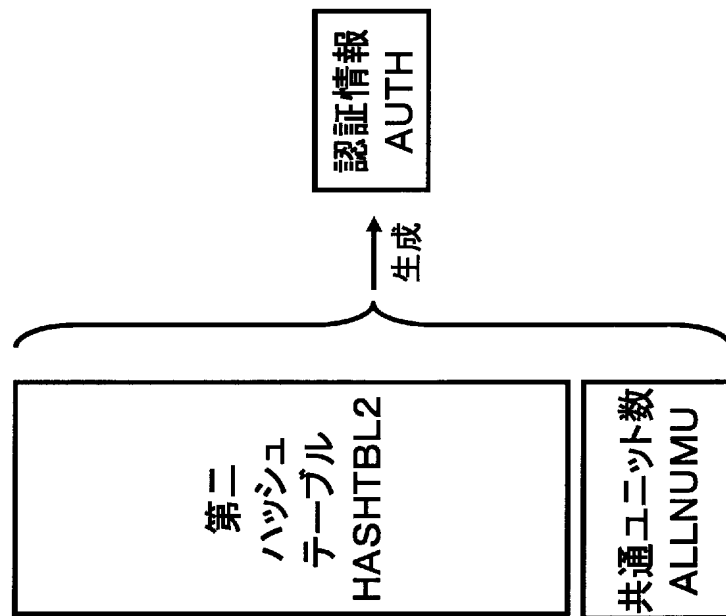
暗号化鍵束 KB
第一ハッシュテーブル群 HASHTBL1G
第二ハッシュテーブル HASHTBL2
コンテンツ位置情報 POS
配布データ領域特定情報 AREA
実行手順データ NAV
認証情報 AUTH
暗号化コンテンツ ENCNT



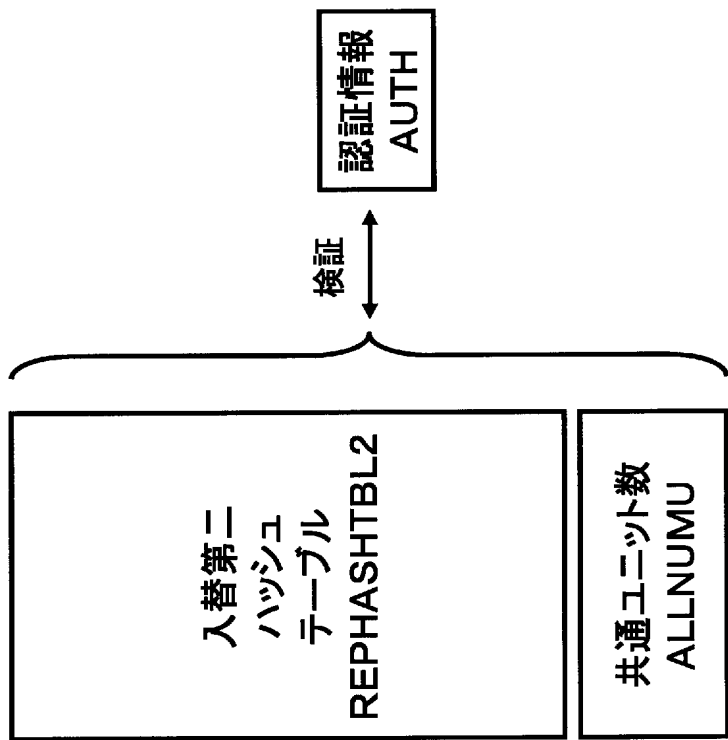
コンテンツ位置情報 POSの別の一例



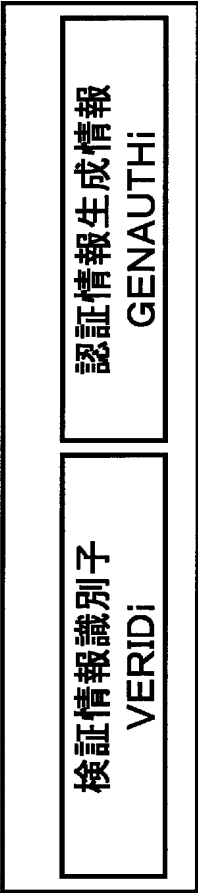
認証情報AUTHの作成方法の別の一例



認証情報AUTHの検証方法の別の一例



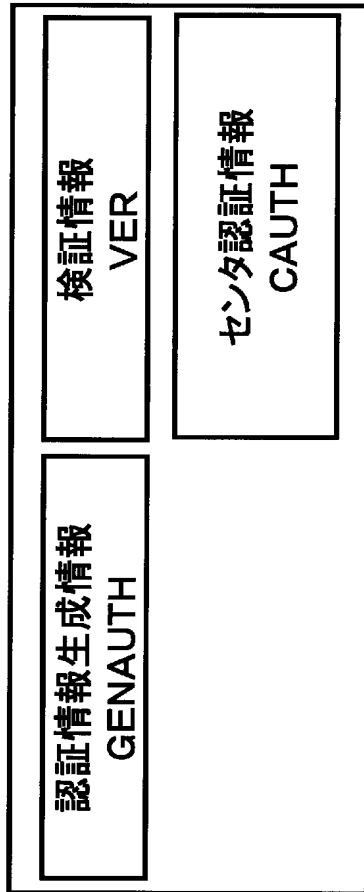
認証情報生成情報格納部1009の別の一例



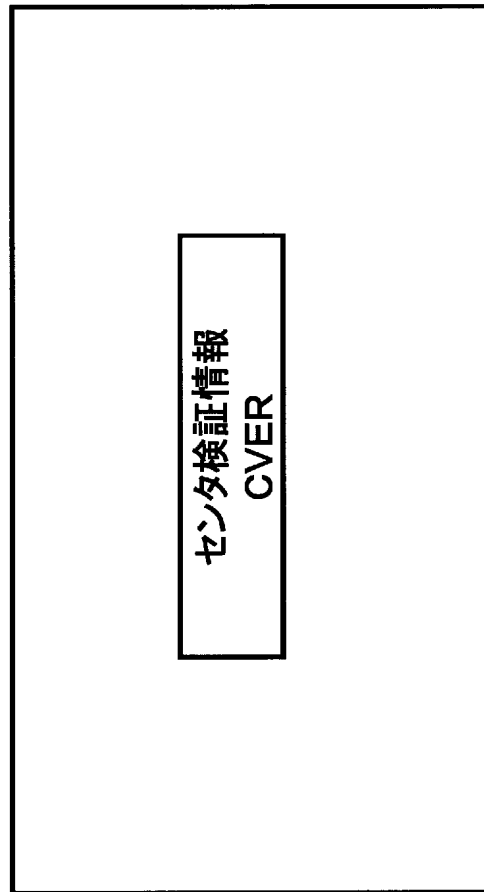
検証情報格納部1215の別の一例

検証情報識別子 VERID1	検証情報 VER1
検証情報識別子 VERID2	検証情報 VER2
▪ ▪ ▪	▪ ▪ ▪
検証情報識別子 VERIDw	検証情報 VERw

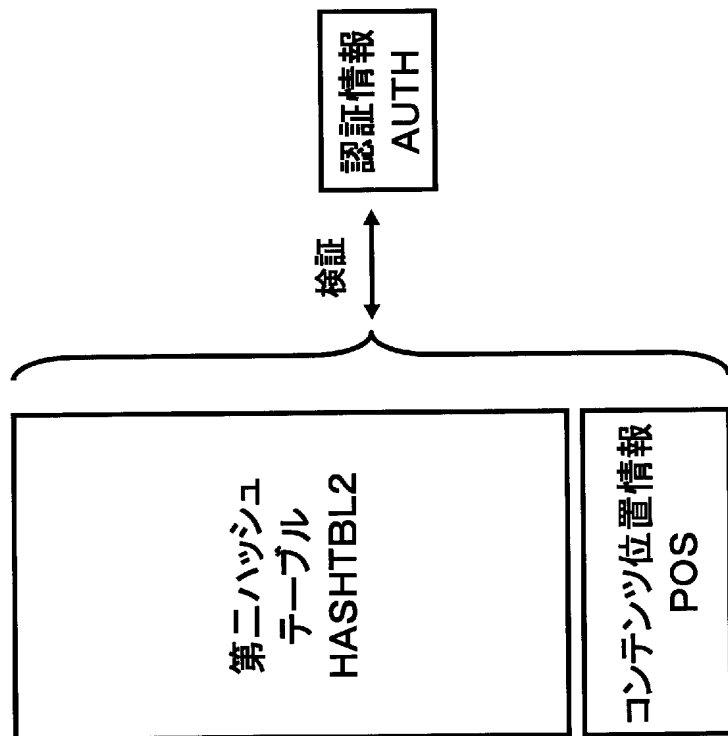
認証情報生成情報格納部1009の別の一例



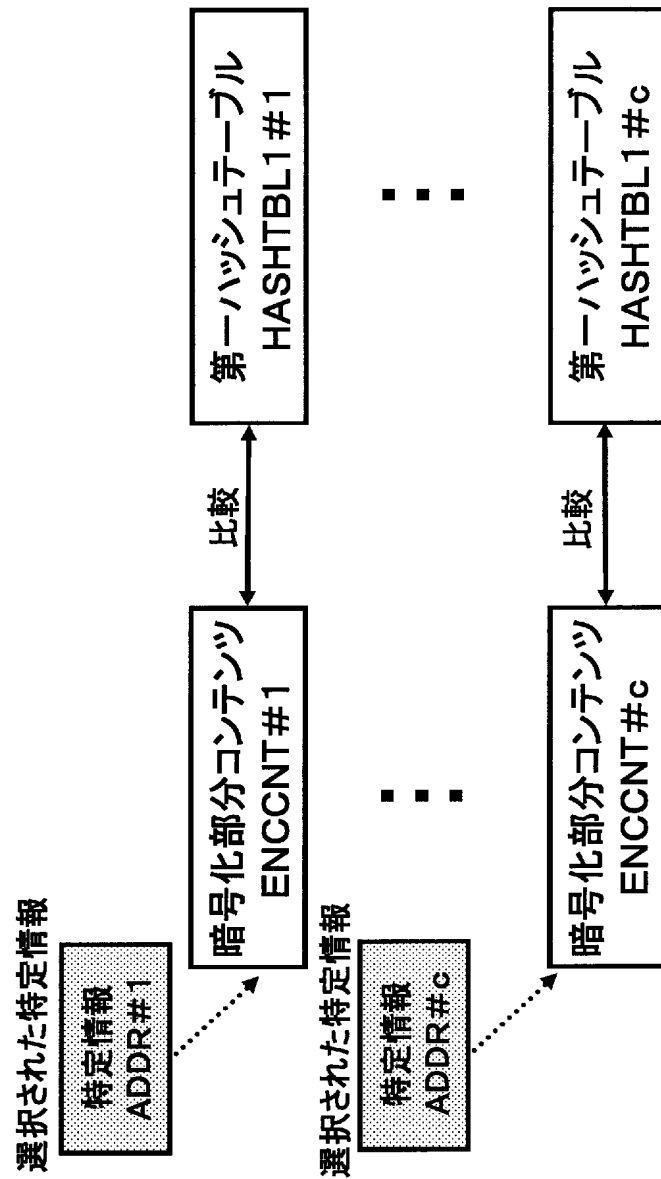
検証情報格納部1215の別の一例



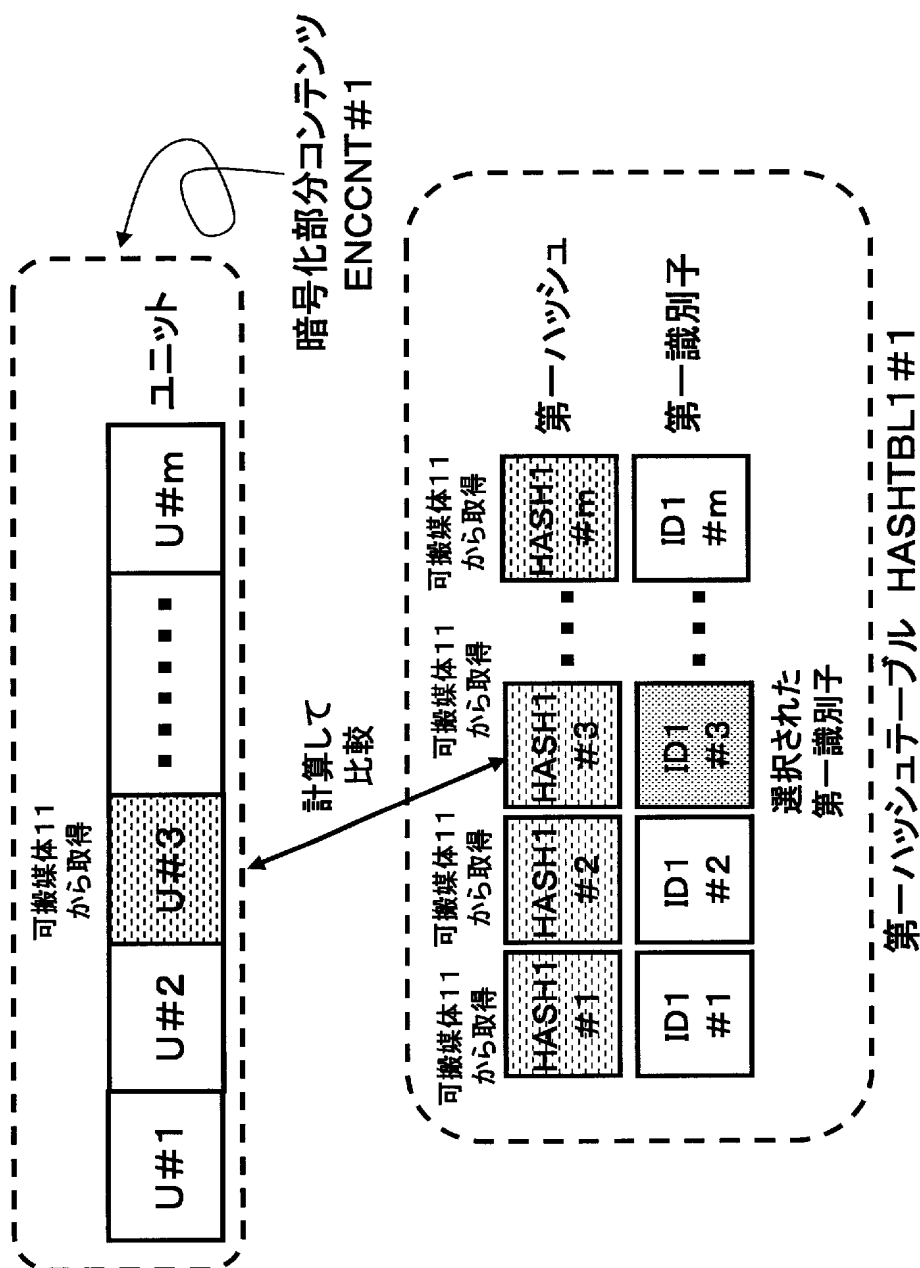
認証情報AUTHの別の検証例(ステップ1)



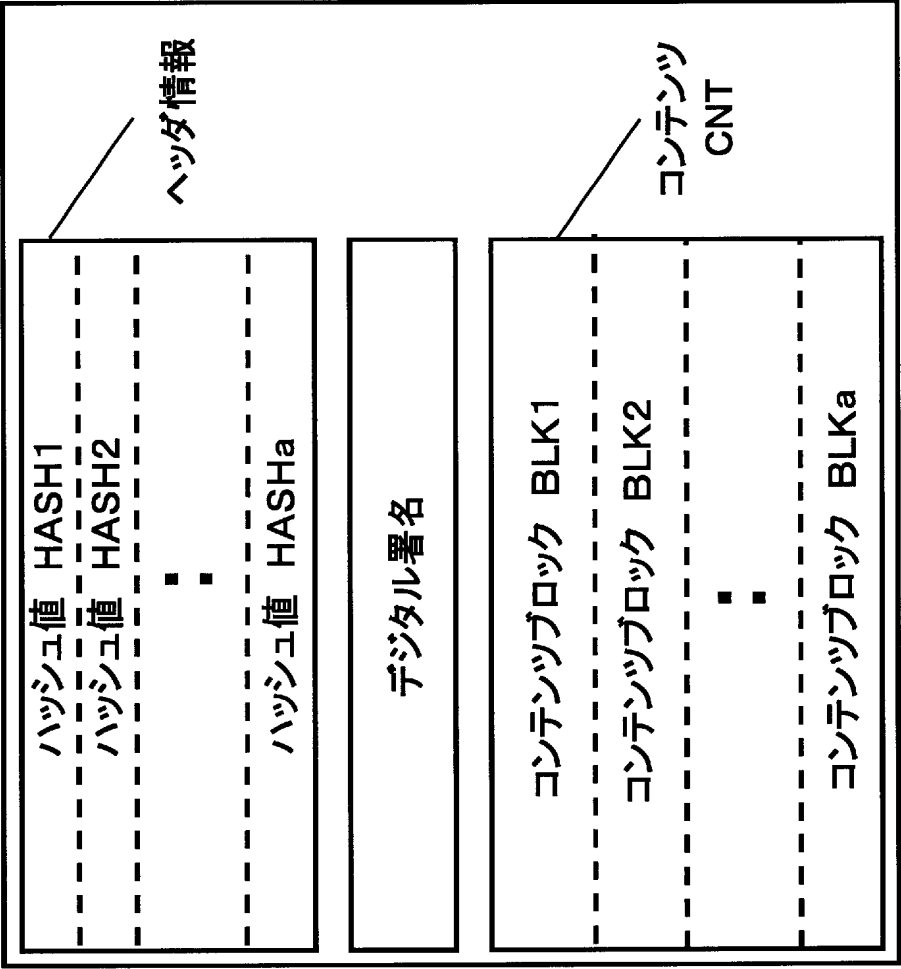
認証情報AUTHの別の検証例(ステップ2)



認証情報AUTHの別の検証例(ステップ2の詳細2)



従来技術の可搬媒体に記録されるデータ



【書類名】 要約書

【要約】

【課題】 実行装置において不正コンテンツかどうか検知することが出来なかった。

【解決手段】 配布センタ１０が、コンテンツＣＮＴとともに、そのコンテンツの領域を特定する配布データ領域特定情報と、配布データ領域特定情報を含む検証対象データに対する認証情報AUTHを可搬媒体１１に記録し、実行装置１２では、コンテンツＣＮＴの実行、再生開始前に、認証情報AUTHが正規の認証情報であるか検証し、検証結果が正当な場合にのみ、配布データ領域特定情報を基に配布データを特定し、配布データのみを実行する。

【選択図】 図１

出願人履歴

0 0 0 0 0 5 8 2 1

19900828

新規登録

大阪府門真市大字門真 1 0 0 6 番地

松下電器産業株式会社